UNIVERSIDADE DE TAUBATÉ

Melissa Giovana Ananias Magalhães

COMPLIANCE:
o Impacto da Lei Geral de Proteção de Dados

Taubaté

2023

Melissa Giovana Ananias Magalhães

COMPLIANCE:
o Impacto da Lei Geral de Proteção de Dados

Trabalho de graduação apresentado para obtenção do certificado de bacharel pelo Curso de Direito do Departamento de Ciências Jurídicas da Universidade de Taubaté.
Área de concentração: Lei Geral de Proteção de Dados.
Orientação: Professor Me. Avelino Alves Barbosa Júnior.

Taubaté

2023

Grupo Especial de Tratamento da Informação - GETI
Sistema Integrado de Bibliotecas - SIBi
Universidade de Taubaté - UNITAU

M189c Magalhães, Melissa Giovana Ananias
Compliance : o impacto da lei geral de proteção de dados / Melissa Giovana Ananias Magalhães. -- 2023.
61f.

Monografia (graduação) - Universidade de Taubaté, Departamento de Ciências Jurídicas, 2023.
Orientação: Prof. Me. Avelino Alves Barbosa Júnior, Departamento de Ciências Jurídicas.

1. Lei geral de proteção de dados. 2. Compliance. 3. Direito à privacidade. I. Universidade de Taubaté. Departamento de Ciências Jurídicas. Curso de Direito. II. Título.

CDU - 343.45:004.738.5(81)

Ficha catalográfica elaborada pela Bibliotecária Regina Márcia Cuba – CRB 8ª/7416

MELISSA GIOVANA ANANIAS MAGALHÃES

COMPLIANCE: O IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de graduação apresentado para obtenção do certificado de bacharel pelo Curso de Direito do Departamento de Ciências Jurídicas da Universidade de Taubaté.

Data: _____

Resultado: _____

BANCA EXAMINADORA

Professor Me. Avelino Alves Barbosa Júnior, Universidade de Taubaté.

Assinatura _____

Professor _____, Universidade de Taubaté.

Assinatura _____

Dedico este trabalho à minha avó, Leonor (*In Memorian*), em razão de todos os ensinamentos que sua sabedoria foi capaz de me transmitir.

AGRADECIMENTOS

Chega ao fim à graduação, parte de um ciclo iniciado ainda na pré-escola, o qual, por ora, mostra-se finalizado. Afirmo, com certeza, que os conhecimentos adquiridos nesses anos serão importantes para o resto de minha vida. Agradeço profundamente cada professor que me acompanhou nesse trajeto, mas em especial, agradeço aqueles que foram capazes de ministrar conhecimentos que ultrapassam a vida acadêmica e profissional.

Agradeço a minha Mãe, Sandra, que fazendo papel de mãe e pai, me acompanhou nos momentos mais importantes de minha vida, e em todas as vezes que pensei em desistir, me incentivou, acreditando mais em mim do que eu mesma consigo acreditar.

Agradeço a minha família, pelo carinho, incentivo e ajuda me dada nesses anos, estar próximo a vocês me faz sentir a pessoa mais afortunada desse mundo.

Agradeço a todos os meus amigos, em especial à Larissa, Thalita e ao Vinicius, que fizeram esse trajeto ser mais divertido e leve. O restante, não citarei nominalmente, mas cada um possui importância ímpar.

Agradeço, ainda, todos àqueles que direta ou indiretamente contribuíram para o meu aprendizado, seja dentro ou fora da graduação.

Por fim, agradeço a mim. Ao que fui. Ao que sou. Ao que ainda serei.

“Uma máquina consegue fazer o trabalho de 50 homens ordinários. Nenhuma máquina consegue fazer o trabalho de um homem extraordinário”.

(Elbert Hubbard)

RESUMO

O presente trabalho de graduação possui o objetivo de analisar os programas de *Compliance* para adequação das empresas à Lei Geral de Proteção de Dados. A relevância do tema encontra-se nos danos que a insegurança do avanço tecnológico vem causando à população, o que acontece especificamente pelo número de informações veiculadas nos sistemas informatizados. Para isso, é imprescindível pontuar os momentos históricos que antecederam a LGPD, o contexto que deu causa a sua promulgação, bem como delimitar o tema privacidade. Objetivou-se expor os principais pilares dos programas de *Compliance*, demonstrando sua importância e requisitos. Constata-se, ainda, que a LGPD é um grande salto para o ordenamento jurídico, entretanto está longe de ser suficiente, por isso a importância dos programas de *Compliance* – aliado das empresas e dos titulares de dados. Quanto à sistematização, far-se-á o uso do método dialético, e desenvolver-se-á o trabalho principalmente por meio de pesquisa bibliográfica com base em artigos, doutrinas e leis.

Palavras-chave: proteção de dados; *compliance*; privacidade;

ABSTRACT

This monograph objective is to analyze Compliance programs to adapt companies to the General Data Protection Law. The relevance of the topic lies in the damage that the insecurity of technological advances has caused to the population. To achieve the objective, is essential to highlight the historical moments that preceded the GDPL and the context that led to its promulgation, as well as delimiting the topic of privacy. The objective was to expose the main pillars of Compliance programs, demonstrating their importance and requirements. It is also clear that the GDPL is a great leap forward for the legal system, nonethless it is far from being sufficient, hence the importance of Compliance programs – an ally of companies and data holders. As for systematization, the dialectical method will be used, and the work will be carried out mainly through bibliographical research based on articles, doctrines and laws.

Keywords: data protection; compliance; privacy;

LISTA DE ABREVIATURAS E SIGLAS

ANPD: Autoridade Nacional de Proteção de Dados

CPF: Cadastro de Pessoa Física

CDC: Código de Defesa do Consumidor

FCPA: Foreign Corrupt Practices Act

GDPR: General Data Protection Regulation

LAI: Lei de Acesso à Informação

LGPD: Lei Geral de Proteção de Dados

SNI: Serviço Nacional de Informações

UE: União Europeia

SUMÁRIO

1 INTRODUÇÃO

Notoriamente a sociedade contemporânea experimenta, a cada dia, evoluções tecnológicas que antes eram inimagináveis. O termo “notoriamente”, utilizado na oração anterior, faz-se necessário porque a evolução da tecnologia é, de fato, perceptível aos olhos de qualquer ser humano capaz. A título de entendimento e contextualização, cita-se a Terceira Revolução Industrial ocorrida na metade do Século XX, ocasião onde à chegada da informática, robótica e telecomunicação provocou o melhoramento de invenções antigas e possibilitou à criação de novos equipamentos, quais sejam: robôs, computadores e televisores (Dias, 2018).

A partir daí, a vida da população tem se tornado cada vez mais prática, pois quase tudo pode ser feito à distância. Basta um *click*. Nessa toada, os melhoramentos que a tecnologia e a internet trouxeram para o mundo moderno foram capazes de ocasionar uma série de mudanças nas relações interpessoais e socioeconômicas. Nota-se que atualmente a tecnologia é pertencente ao mundo moderno, de maneira que viver sem esse instrumento pode se tornar angustiante ou demasiadamente difícil, não somente para as gerações mais novas que nasceram moldadas a esse universo, mas também para os mais velhos que, de certa forma, já se habituaram a esse ambiente.

As pesquisas são capazes de confirmar, o número de pessoas inteiradas com o meio tecnológico vem crescendo, inclusive entre aqueles de idade mais avançada: “[...] o percentual de utilização dos idosos foi o que mais aumentou: de 44,8% para 57,5%, alta de 12,7 pontos percentuais, superando, pela primeira vez, os 50%” (Brito; Nery, 2022, *online*). Em uma perspectiva geral: “de janeiro de 2015 a janeiro de 2020, o número de brasileiros usuários de Internet aumentou de 110 milhões para 150,4 milhões” (Cominetti, 2021, p. 17).

Ocorre que isso possui consequências que precisam ser observadas. “Com tantos usuários ativos, a quantidade de dados coletados por essas redes sociais é considerável. Sendo parte deles sensíveis, são fornecidos livremente e sem preocupação pelos participantes da plataforma” (COMINETTI, 2021, p. 17).

Para regular as relações jurídicas decorrentes do uso dessas informações, surge a Lei Geral de Proteção de Dados. Com vários dispositivos, princípios e sanções, sua completa observância pode se tornar trabalhosa, por isso os programas de *compliance* ganharam destaque. Portanto, no presente trabalho

indaga-se a eficácia dos programas de *compliance* como medida apta a tornar adequado o tratamento de dados, assim como previsto na LGPD.

O objetivo geral da pesquisa é, por conseguinte, analisar os principais pontos da LGPD e das normas anteriores a sua vigência, considerando o contexto atual, expondo seus objetivos e a razão pela qual se faz necessária, expondo a importância dos dados, os riscos trazidos pelo seu uso inadequado ou vazamento, bem como as sanções decorrentes dessa prática; por fim, demonstrar a relevância de um programa de *compliance* na área de proteção de dados, explicando seus pilares e sua relação com a LGPD, e apresentando um guia inicial para a adequação das empresas, de acordo com as pesquisas bibliográficas realizadas.

O estudo é relevante, pois se trata de um tema atual e evidente, a proteção de dados, a qual é considerada pelo ordenamento jurídico como um direito fundamental. Logo, qualquer estudo dedicado a esse tema possui relevância, dado seu caráter recente e ainda pouco explorado pelos profissionais do direito. Ainda, cabe mencionar que por ser recente, muito dos estudos relativos a esse tema ainda são rasos ou incompletos, portanto, através desse trabalho, pretende-se contribuir, ainda que minimamente, para a conscientização acerca do assunto.

Como metodologia, adotou-se a pesquisa bibliográfica mediante leitura crítica, resumos e paráfrases das obras pertinentes ao tema. Segue, por fim, a conclusão e as referências.

2 CONTEXTO HISTÓRICO AO REDOR DO MUNDO

Durante todo o tempo, a internet é capaz de cruzar diversos tipos de elementos, de variadas pessoas, a fim de realizar tarefas ditas sensacionais; mas quase ninguém se submete a reflexão dos danos, muitas das vezes irreparáveis, causados pelo eventual emprego inadequado dessas informações. Entretanto, aquele que teve seus dados vazados na internet, sabe bem as consequências causadas por esse vazamento, os quais vão além da esfera individual e não se limitam aos acostumados danos morais ou patrimoniais. Inclusive, esses danos são capazes de atingir o coletivo, como no caso *Cambridge Analytica*[1]. A título de exemplificação, Cominetti (2021, p. 19), em sua obra, faz um comentário que se amolda perfeitamente a esse famoso acontecimento: “as plataformas que proveem esse serviço adquiriram um grande poder, capaz, inclusive, de influenciar em resultados de votações de grande relevância para o cenário mundial”.

Portanto, pode se dizer que, embora repleta de benefícios, a tecnologia, por vezes, será nociva. E essa nocividade é fruto, em parte, da violenta velocidade com que a informação transita nos meios digitais. Cueva (2016, p. 9) explica:

> A obtenção e a disseminação massificada e praticamente instantânea dessas informações, cujo conteúdo nem sempre constitui um segredo nem caracteriza uma invasão de privacidade, no sentido clássico que se atribui a este direito, põem em xeque a efetividade da tutela jurídica da vida privada, pois os indivíduos são despojados do direito de participar e de algum modo controlar as informações que sobre eles são produzidas e divulgadas, e evidenciam uma crise na própria noção de intimidade (Cueva, 2016, p. 9).

É aí que surge a exigência de toda uma restruturação tanto da sociedade, como das ciências, nesse caso em específico, das ciências jurídicas, a qual se compromete com as normas jurídicas aplicadas à sociedade. “[...] é indispensável promover reflexões voltadas aos problemas jurídicos advindos da evolução tecnológica, principalmente os decorrentes da massificação do uso da internet” (Boff; Fortes, 2014, p. 114). Assim, há de ser concretizada uma nova cultura capaz de conscientizar a população, com o interesse principal de reduzir os transtornos causados pela tecnologia.

Nas palavras de Pinheiro (2021, p. 17):

---

[1] **Cambridge Analytica:** trata-se de um caso que envolveu a coleta indevida de informações pessoais de 87 milhões de usuários do Facebook sem o seu conhecimento ou consentimento, e o uso desses dados foram usados para influenciar a opinião pública durante as eleições presidenciais dos Estados Unidos em 2016 (G1, *online*).

> É importante compreender que vivemos um momento único, tanto no aspecto tecnológico como no econômico e social. O profissional de qualquer área, em especial o do Direito, tem a obrigação de estar em sintonia com as transformações que ocorrem na sociedade. Sabemos que o nascimento da Internet é um dos grandes fatores responsáveis por esse momento, mas o que é fundamental, antes de tudo, é entender que esses avanços não são fruto de uma realidade fria, exclusivamente tecnológica, dissociada do mundo cotidiano (Pinheiro, 2021, p. 17).

Logo, há ânsia em regulamentar as relações jurídicas provenientes da internet, urge a indispensabilidade de estar seguro em meio a tanta inteligência. É nesse contexto que surge a *General Data Protection Regulation* – GDPR, que acabou por inspirar outras legislações, como a Lei Geral de Proteção de Dados – LGPD, lei brasileira, instrumento desse trabalho, a qual terá um capítulo específico explicando seus principais pontos. Por ora, cabe indagar-se: será que a preocupação com a exposição causada pela tecnologia é uma problemática exclusiva dos dias atuais? Não, muito pelo contrário.

Embora a preocupação com a privacidade e proteção de dados tenha ganhado destaque nos últimos anos, essa não é uma problemática exclusiva do século XXI:

> O início dos debates doutrinários sobre o direito à privacidade ocorreu como consequência da utilização de novas técnicas e instrumentos tecnológicos, que passaram a possibilitar o acesso e a divulgação de fatos relativos à esfera privada do indivíduo de uma forma anteriormente impensável. Isso pode ser percebido com o pioneiro artigo sobre privacidade de *Warren* e *Brandeis*, intitulado "*The right to privacy*", no qual os autores denunciavam como a fotografia, os jornais e aparatos tecnológicos tinham invadido os sagrados domínios da vida privada e doméstica. (Mendes, 2014, p. 27).

Portanto, segundo diversos autores, a privacidade foi objeto de preocupação pela primeira vez ainda no século XIX, através de um artigo escrito por *Warren* e *Brandeis* – *The Right Privacy*. Já o primeiro diploma encarregado pela manutenção da privacidade, a Declaração Universal dos Direitos Humanos, surgiu em 1948.

Dito isso, tem-se adiante uma breve abordagem dos fatos históricos e dos principais diplomas encarregados pela revisão da privacidade e da proteção de dados. Desde o primeiro registro que se tem conhecimento até os últimos dias, a começar pelo *Right to Privacy*.

2.1 *The Right to Privacy*

Conforme explica o dicionário *online,* o termo privacidade remete-se a noção de intimidade pessoal da vida particular. O que, se traduzido para a língua inglesa,

torna-se *privacy*. E a ideia de *privacy* surge ainda no século XIX, nos Estados Unidos. Segundo Zanini (2017), nessa época um determinado indivíduo teria manifestado o desejo de "ser deixado só", o que lhe foi concedido sem grandes repercussões. Isso, pois, tal fato só viria a repercutir anos depois, por intermédio do artigo *The Right to Privacy,* escrito por Samuel D. Warren e Louis D. Brandeis.

Publicado em 1890, ele menciona diversas transformações e inovações, a exemplo da fotografia, que provocaram a violação da esfera pessoal dos seres humanos, surgindo, portanto, a necessidade de defender o "direito de estar só" (Zanini, 2017).

Soma (*apud* Zanini, 2017, p. 233) explica:

> Os autores partem desses problemas para analisar um bom número de decisões de tribunais ingleses e americanos, deduzindo então a existência de um princípio geral na Common Law, o *right of privacy*. Assim, utilizando a expressão *right to be let alone*, propõem um novo *tort*, a invasão do *privacy*, que constituiria uma profunda ofensa, a qual lesionaria o senso da própria pessoa sobre sua independência, individualidade, dignidade e honra. (Soma; *apud* Zanini, 2017, p. 233).

Esse artigo foi essencial para o desdobramento da temática abordada, e principalmente, para o alcance do reconhecimento de um direito à privacidade, causando reflexos positivos nos ordenamentos jurídicos de diversos continentes (Miranda, 2013). Conclui-se, portanto, que o direito à privacidade surge pela primeira vez, ainda que superficialmente, através da jurisprudência norte-americana (Reinaldo Filho, 2013).

2.2 Declaração Universal dos Direitos do Homem

De outro lado, Carloto (2021) ensina que o direito à privacidade foi reconhecido pela primeira vez na Declaração Universal dos Direitos do Homem (DUDH), já em 1948:

> Art. 12: Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. (UNICEF, *online*).

Segundo ela, a Declaração Universal dos Direitos do Homem foi importante porque surgiu como resposta aos abusos cometidos durante a primeira e segunda guerra mundial. Ao encontro, Ricardo Alexandre de Oliveira (2018) leciona que as pessoas mortas nessa ocasião foram perseguidas e executadas em decorrência de

suas convicções política, religiosa ou até mesmo pela orientação sexual; por sua vez, essas informações dizem respeito à intimidade e privacidade do indivíduo, daí se extrai a necessidade de positivar a proibição de interferência na esfera pessoal dos indivíduos.

Hirata (2017) concorda e aponta outros instrumentos que surgiram na mesma época e que também possuíam o objetivo de conferir guarida ao direito de privacidade, dentre os quais podemos citar a 9ª Conferência Internacional Americana de 1948, a Convenção Europeia dos Direitos do Homem de 1950, a Conferência Nórdica sobre o Direito à Intimidade, de 1967, o Pacto San Jose da Costa Rica, de 1969, além de outros documentos internacionais.

A Declaração Universal dos Direitos do Homem é vista, então, como o primeiro instrumento que positiva o direito a privacidade.

2.3 Lei de Hesse

Agora, já no tema específico de proteção de dados, tem-se que esse foi tratado pela primeira vez na década de 70. Nessa época, no continente Europeu, houve uma revolução tecnológica que exigiu a criação de uma disciplina de proteção de dados. Então, com intermédio do jurista Spiros Smitis, o Estado de Hesse, na Alemanha, inaugurou uma lei com o intuito de regular a proteção de dados no âmbito local (Tommaso, 2020, *online*).

Atualmente, percebe-se que, mesmo tendo sido construída há décadas, a lei de Hesse já trazia consigo conceitos modernos, ainda muito utilizados. “Sua primeira versão já abordava, cinco décadas atrás, questões como sigilo, controle de acesso, armazenamento, transferência de dados, modificação ou destruição ilegal de dados e até mesmo o direito ao acesso do titular aos seus dados” (Tommaso, 2020, *online*).

A partir disso, não demorou muito para que a circulação de dados se tornasse preocupação para outras regiões, surgindo, em 1981, a Convenção n° 108 do Conselho Europeu.

2.4 Convenção n° 108 do Conselho Europeu

Retratada como o primeiro tratado capaz de produzir efeitos que ultrapassaram o cenário europeu, a convenção zela pelo direito à vida privada frente ao tratamento robotizado dos dados pessoais. Não somente isso, ela é conceituada no mundo todo como uma das mais relevantes ocorrências relacionadas ao tema (Camargo; Fanchinetti, 2021, *online*).

Logo no primeiro artigo, a convenção estabelece seus objetivos e finalidades:

> Artigo 1 – objeto e finalidade: a presente Convenção tem por finalidade proteger todas as pessoas, independentemente da sua nacionalidade ou residência, no que diz respeito ao tratamento dos seus dados pessoais, contribuindo assim para o respeito dos seus direitos humanos e liberdades fundamentais e, em especial, do direito à vida privada (França, 1981).

Assim como a Lei de Hesse, a convenção também trata de definições interessantes, como dados pessoais, ficheiro automatizado, tratamento automatizado e ainda define quem é o responsável pelos ficheiros.

> Artigo 2 – Definições Para os efeitos da presente Convenção:
> a. “dados pessoais” refere-se a qualquer informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”);
> b. “tratamento de dados” refere-se a qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, tais como a recolha,armazenamento, preservação, alteração, recuperação, divulgação, disponibilização, supressão, destruição ou execução de operações lógicas e/ou aritméticas sobre esses dados;
> c. Caso não seja utilizado o tratamento automatizado, “tratamento de dados” refere-se a uma operação ou a um conjunto de operações efetuadas sobre dados pessoais no âmbito de um conjunto estruturado desses dados, acessíveis ou recuperáveis de acordo com critérios específicos;
> d. “responsável pelo tratamento” refere-se à pessoa singular ou coletiva, autoridade pública, serviço, agência ou qualquer outro organismo que, individualmente ou em conjunto com outros, tenha poder de decisão em matéria de tratamento de dados;
> e. “destinatário” refere-se à pessoa singular ou coletiva, autoridade pública, serviço, agência ou qualquer outro organismo a quem sejam comunicados ou disponibilizados dados;
> f. “subcontratante” refere-se a uma pessoa singular ou coletiva, autoridade pública, serviço, agência ou qualquer outro organismo que trate dados pessoais por conta do responsável pelo tratamento (França, 1981).

A convenção é baseada em três principais pilares “[...] proposta de dispositivos legais substanciais apresentados como princípios basilares à proteção de dados, regras específicas para a transferência de dados transfronteiriços e mecanismos de assistência mútua e consulta entre os signatários”. (Camargo; Fanchinetti, 2021, *online*). Atualmente a convenção conta com 55 membros e oito países observadores, dentre eles, o Brasil (Camargo; Fanchinetti, 2021, *online*).

2.5 Diretiva 95/46/CE

Em 1995, o Parlamento Europeu aprovou a Diretiva 95/46/CE. Apresentando de maneira sintética, a Diretiva exigiu uma agência de proteção de dados em cada país integrante da União Europeia (UE), assim como determinou que cada país editasse sua própria lei para processamento das informações, unificando a coleta e o tratamento de dados, o que deveria ocorrer em até três anos de sua publicação (Reinaldo Filho, 2013). Mendes (2014) explica, ainda, que há uma imensa semelhança entre as nomenclaturas presentes na Convenção 108, na Diretiva 95/46/CE e no artigo 5º da atual Constituição.

A Diretiva, embora muito útil, assim como os outros diplomas, já não era mais capaz de acompanhar os avanços da tecnologia e do mundo sociopolítico. Em razão disso, em 2018 entra em vigor o Regulamento Geral sobre Proteção de Dados, também conhecida como GDPR.

2.6 *General Data Protection Regulation*

A GDPR surge ainda em 2016, por intermédio do partido *The Greens*, da União Europeia. Seu objetivo é versar sobre a proteção de dados de pessoas físicas, especificamente no que se refere a livre circulação desses dados. Através de grande repercussão, entra em vigor em 2018, após dois anos de adequação, iniciando-se então, a aplicação das penalidades (Pinheiro, 2023).

A GDPR foi capaz de encadear um efeito cascata, já que exigiu dos demais países a necessidade de também se adequarem com uma legislação do mesmo nível, vez que, na lei, há exigência de que os estados membros da União Europeia somente comercializem com países que manifestem seriedade em relação ao tratamento de dados dos seus cidadãos (Araújo; Santos, 2021). Dito isso, aduz Pinheiro (2023, p. 10) “considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina, não poderia se dar”.

E a com a finalidade de não ser prejudicado nessa relação, surge, no Brasil, a Lei Geral de Proteção de Dados (LGPD), publicada em 14 de agosto de 2018 e fortemente inspirada na GDPR.

Cabe esclarecer que a LGPD será objeto de outro tópico neste instrumento, preocupando-se, até aqui, apenas com apresentar ao leitor os atos que sucederam a GDPR e a LGPD.

3 CONTEXTO HISTÓRICO NO BRASIL – JURISPRUDÊNCIA

No Brasil, a privacidade, compatível minimamente com o que se conhece hoje, surge através da jurisprudência, nos anos 90. Há um primeiro acórdão julgado pelo STF (RHD 22/DF, Pleno, j. 19-9-1991, m.v., rel. Min. Marco Aurélio, rel. p/ acórdão Min. Celso de Mello, DJ 1o-9-1995), em uma ação de *habeas data*, onde o impetrante pretende ter acesso aos seus dados pessoais, presente nos ficheiros do extinto Serviço Nacional de Informações – SNI. Nesse julgamento, fica constatada a associação entre o *habeas data* e o direito de acesso aos dados pessoais, conforme prevê a Constituição (Mendes, 2014).

Ressalta-se que não faltam julgados respaldados na constituição com a finalidade de obter a proteção aos dados, mas o objetivo deste instrumento não é mencionar um a um, e sim realizar uma breve menção a respeito dos fatos influentes neste cenário.

Dito isso, nota-se que a jurisprudência, baseada nos padrões constitucionais, foi importantíssima para a evolução do direito à privacidade no ordenamento brasileiro, especialmente quando ainda não existiam outras normas capazes de regular essa situação, até o espaço tempo da aparição do Código de Defesa do Consumidor (CDC) ou de outras normas legais e infralegais (Mendes, 2014).

3.1 Código de Defesa do Consumidor – Lei Nº 8.078/1990

Aprovado em 1990, o Código de Defesa do Consumidor (CDC) surge em uma época honrosa, marcada pela redemocratização ante a aprovação da Constituição cidadã, responsável por trazer à tona a valorização da pessoa humana (Carpena, 2020, *online*). Sua principal ideia é a proteção do consumidor e isso pode ser observado a partir da leitura do art. 4°, *caput*, do referido diploma:

> Art. 4°: A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo [...] (Brasil, 1990).

O CDC possui diversos objetivos, dentre os quais se destacam: a proteção dos consumidores - vulneráveis relativamente às grandiosas empresas conhecidas

pelas práticas abusivas; o direito à informação clara e adequada e o direito à segurança e qualidade dos serviços oferecidos (Pessoa, 2023, *online*).

Apontado como a primeira legislação a tratar da privacidade e proteção de dados de um jeito moderno - sob a ótica dos avanços tecnológicos – o CDC se torna importantíssimo, já que a partir da vigência, a tutela da privacidade passou a ser regulada além da Constituição e da jurisprudência, estendendo-se a outras normas (Mendes, 2014). Por isso, alguns autores chegam até a igualar o CDC e a LGPD em grau de importância:

> Cabe perfeitamente a comparação. Cada lei é produto de seu tempo e, se o fim do século XX foi marcado pelo fenômeno do consumo, não resta dúvida de que o início do atual se caracteriza pela onipresença da tecnologia digital em nossas vidas, não apenas nos objetos e na forma com que passamos a consumir, mas, sobretudo como mediadora das relações sociais e como via de construção das identidades. (Carpena, 2020, *online*).

É relevante lembrar que o CDC, em seu art. 43, chega a dispor sobre a regulamentação dos bancos de dados referentes aos cadastros dos consumidores:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
> § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor (Brasil, 1990).

Uma das pertinências desse dispositivo mora no fato de que: “o código autoriza o funcionamento dos bancos de dados e cadastros de consumidores, desde que atendidos determinados preceitos para a proteção da privacidade dos consumidores” (Mendes, 2014, p. 142).

Outro ponto a ser considerado nesse mesmo artigo, é a obrigação de que o uso e coleta dos dados sejam submetidos ao crivo da legalidade: “a lei determina

que os bancos de dados e cadastros relativos a consumidores são considerados públicos e, portanto, devem respeitar os limites legais" (Mendes, 2014, p. 143). Por conta disso é que ele aponta também pela ineficácia da argumentação – por parte das empresas - que os dados coletados serão usados para fins particulares não submetidos à legislação; para isso, estabelece que os dados dizem respeito à personalidade do consumidor – não sendo exclusividade da empresa, e sim do público - e, portanto, devem ser submetidos ao regime constitucional. E o meio adequado para fazer essa queixa, é o *habeas data* (Mendes, 2014).

3.2 *Habeas Data* – Lei N° 9.507/1997

Trata-se de um remédio constitucional gratuito, previsto pela primeira vez na Constituição Federal de 1988. "Seu étimo advém da palavra latina *habeas*, cujo significado é tenhas em tua posse, e *data*, que denota o sentido de base de dados". (Canotilho et al., 2018, p. 519). Sua principal função é garantir os direitos individuais e coletivos:

> Esta sua posição no ordenamento deve ser entendida no âmbito de uma reação, que se deu no momento em que a sociedade e o próprio ordenamento se recompunham de um período no qual diversas liberdades individuais foram suprimidas. Neste contexto, o *Habeas Data* foi uma das medidas destinadas a sanar um "déficit" de liberdades individuais, bem como de consolidar as bases democráticas do novo sistema e dificultar uma volta a um regime ditatorial (Doneda, 2008, p. 21).

O *habeas data*, inspirado nas legislações portuguesas e espanholas, surgiu para defender o direito à informação e frear a transmissão de dados, já que, o Estado, influenciado por motivações políticas durante a ditadura, cometeu diversos desrespeitos à individualidade das pessoas (Canotilho et al., 2018). Em harmonia, Doneda (2008) declara que o Brasil foi um dos primeiros países a ver introduzido em seu ordenamento jurídico o *habeas data*, mas apesar disso, nenhuma evolução ulterior, no âmbito da disciplina de dados, foi alcançada - gerando certo paradoxo.

De fato, da leitura do artigo 5°, LXXII, depreende-se que o legislador buscou proteger o cidadão de possíveis transgressões cometidas pelo Estado, no que diz respeito às informações armazenadas em bancos de dados (Doneda, 2008).

> LXXII - conceder-se-á *"habeas-data":*
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo (Brasil, 1988).

O *habeas data* visa assegurar um direito presente em nosso ordenamento jurídico, e como consequência, possibilita que os impetrantes exijam do coato a revelação das informações pertinentes e, sendo essas inexatas, reivindique que o mesmo proceda à sua retificação (Doneda, 2008). É isso que estabelece a lei do *habeas data*:

> Art. 7° Conceder-se-á *habeas data*:
> I - para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público;
> II - para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;
> III - para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro, mas justificável e que esteja sob pendência judicial ou amigável (Brasil, 1997).

Arrematando, é possível notar que o *habeas data*, assim como o CDC, apesar de ser um importante diploma, não é capaz de tutelar, efetivamente e por si só, a proteção de dados pessoais do mesmo modo que a LGPD. E por obvio, como já elucidado, isso ocorre porque cada legislação é fruto das necessidades do seu tempo (Carpena, 2020, *online*).

3.3 Código Civil – Lei N° 10.406/2002

Em vigor desde 2003, o Código Civil (CC) traz no capítulo dos direitos da personalidade um artigo dedicado à privacidade: “art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (Brasil, 2002).

Segundo Ricardo Alexandre de Oliveira (2018), o CC contribuiu grandemente para a proteção da privacidade, pois ele a reconhece como direito intransferível e irrenunciável. Por outro lado, Laura Schertel Mendes (2014), explica que esse é o único artigo do código dedicado à privacidade, o qual, segundo ela, além de ser insuficiente, trata-se, na verdade, de uma cópia daquilo que já foi registrado na Constituição, algo vago e generalista; apesar disso, ela reconhece que, quando interpretado em conjunto com outras normas, esse trecho do código adquire grande relevância.

Essa relevância, explica Mendes (2014), se deve a três fatos. A primeira se deve ao fato de que o dispositivo evidencia a proteção da personalidade em conjunto com a privacidade, o que, conforme ela explica em sua obra, permite a

aplicação das normas constitucionais horizontalmente, ou seja, entre particulares. O segundo ponto a ser observado, é que, por estar inserida no capítulo dos direitos da personalidade, a proteção à privacidade assume o caráter de tutelar a dignidade da pessoa humana. E a terceira observação consiste no fato de que, quando interpretado em conjunto com o CDC (art. 43), o resultado faz surgir um direito à privacidade do consumidor. “Assim, apesar de genérica, a regra tem um grande potencial, que pode ser desenvolvido pelo judiciário e pela doutrina, de modo a se tornar uma efetiva tutela da privacidade e proteção de dados nas relações privadas” (Mendes, 2014, p. 145).

Ainda, de acordo com Oliveira (2018), tanto o CC/02, como a Constituição/88, são ordenamentos generalistas, na sua visão, o CDC é o que melhor se destaca quando o assunto é base de dados.

3.4 Lei Carolina Dieckmann – Lei N° 12.737/2012

A Lei número 12.737/2012 recebe esse nome por conta da grande repercussão alcançada pelo caso da atriz brasileira, Carolina Dieckmann, que teve seu computador invadido por hackers que roubaram diversos dados, inclusive fotos íntimas, que foram publicadas e geraram inúmeros danos (Rocha, 2022, *online*).

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;

> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (Brasil, 2012).

O artigo acima, previsto na lei Carolina Dieckmann, tipifica o crime de "invasão de dispositivo informático", e segundo alguns autores, é o ponto alto da lei. Isso porque acredita-se que ela não foi bem recepcionada e, portanto, não possui grande aplicabilidade na prática (Gonçalves *apud* Rocha, 2022, *online*).

> Em termos práticos, pode-se dizer que não há tanta efetividade, haja vista que, após o seu advento, o próprio legislativo ainda discute inúmeros outros projetos que tratam sobre essa conduta de divulgação de conteúdo íntimo na internet, tendo sido aprovados alguns deles, como por exemplo, a Lei 13. 708/18, que trata sobre a divulgação de fotos, vídeos de nudez ou cenas de sexo como crime no Código Penal Brasileiro. (Gonçalves *apud* Rocha, 2022, *online*).

Além disso, a falta de aplicabilidade se deve também a uma possível rejeição por parte do judiciário, vez que essa norma não foi amplamente debatida antes de entrar vigor, possuindo diversas inconsistências, como "a incerteza sobre o tipo de dispositivo em que o crime pode ser cometido, o que deixa margem para interpretação por partes das autoridades" (Gonçalves *apud* Rocha, 2022, *online*).

Conclui-se, "a lei serve como conduta contra a prática de outros delitos, resolve uma parte do problema que é a invasão de dispositivos, mas não é como poderia ser se tivesse sido mais bem estudada pelo Poder Legislativo" (Gonçalves *apud* Rocha, 2022, *online*).

3.5 Lei do Cadastro Positivo – Lei N° 12.414/2011

A lei do cadastro positivo dispõe sobre o acervo de informações disponíveis em bancos de dados, objetivando construir um histórico de crédito onde se possa consultar a margem de adimplemento e inadimplemento de determinada pessoa natural ou jurídica (Mendes, 2014).

Quando utilizados dessa maneira, pode se perceber que os dados pessoais se tornam protagonistas no mercado de crédito. "Diante da importância que o conhecimento sobre os consumidores adquiriu na economia atual, os dados pessoais tornaram-se capital essencial para o sucesso de inúmeros negócios" (Mendes, 2014, p. 117).

Ressalta-se que esses dados devem ser utilizados única e exclusivamente para fins de concessão de crédito; e tendo em vista que seu principal objetivo é beneficiar o consumidor, informações excessivas e desnecessárias, como as relativas à orientação sexual, convicções políticas, religiosas e filosóficas não podem ser registradas, pois podem gerar discriminação (Mendes, 2014).

> Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
> § 1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado.
> [...]
> § 3º Ficam proibidas as anotações de:
> I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
> II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas. (Brasil, 2011).

E depois, Mendes (2014) alega que essa lei fortalece o direito do indivíduo controlar e proteger seus dados pessoais, pois oferece instrumento para tanto quando lhe concede o poder de cancelar ou reabrir o cadastro se assim desejar:

> Art. 5º São direitos do cadastrado:
> I - obter o cancelamento ou a reabertura do cadastro, quando solicitado;
> II - acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado;
> III - solicitar a impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 10 (dez) dias, sua correção ou seu cancelamento em todos os bancos de dados que compartilharam a informação;
> IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;
> V - ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais;
> VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e
> VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados. (Brasil, 2011).

Para finalizar, cabe mencionar o artigo 16 do referido diploma: “o banco de dados, a fonte e o consulente são responsáveis, objetiva e solidariamente, pelos danos materiais e morais que causarem ao cadastrado [...]”. (Brasil, 2011). Isso importa porque um indivíduo que sofre uma negativação indevida, além de ver restringido seu acesso ao crédito, certamente sofrerá com a fama de mau pagador (Grinover et al., 2019).

> Não bastasse isso, para voltar a ter crédito na praça, encontra inúmeras dificuldades, pois, normalmente, só consegue eliminar os dados negativos existentes a seu respeito, nos bancos de dados, mediante ação judicial, cuja tramitação, como se sabe, em decorrência de vários fatores, é lenta e o resultado, incerto. Assim, a 'negativação' de seu nome nesses arquivos acaba protraindo-se no tempo, com sérios transtornos a sua pessoa, quer na esfera patrimonial, quer na moral. (Grinover et al., 2019, p. 434).

3.6 Lei de Acesso à Informação – Lei N° 12.527/2011

Em vigor desde maio de 2011, a Lei de Acesso à Informação – LAI, objetiva trazer mais transparência à Administração Pública, garantindo ao cidadão acesso às informações públicas (Mendes, 2014). Por óbvio, a LAI possui alguns dispositivos relativos ao tratamento de dados, que serão aqui expostos.

Seu primeiro artigo preceitua:

> Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. (Brasil, 2011).

A partir da leitura, percebe-se que a Lei n. 12.527, possibilita o acesso às informações personalíssimas mantidas pelo Poder Público, prevendo, em outros artigos, prazos e condições para isso (Mendes, 2014). Até aqui se identifica certa semelhança com a legislação do *habeas data*, pois ambas tratam do acesso a informações pessoais. Todavia, Mendes (2014) garante, um não obsta o outro:

> [...] *habeas data*, que é a ação constitucional para acesso, correção e anotação de informações armazenadas em arquivos públicos, não se contrapõe, nem se sobrepõe à lei de acesso à informação. Pelo contrário, ele complementa o direito material de acesso à informação previsto na Lei n. 12.527/2011, na medida em que se constitui como instrumento processual a ser utilizado em caso de descumprimento pela Administração das regras da lei de acesso. (Mendes, 2014, p. 150).

Inclusive, observa-se essa completividade no art. 38 "aplica-se, no que couber, a Lei número 9.507, de 12 de novembro de 1997, em relação à informação de pessoa, física ou jurídica, constante de registro ou banco de dados de entidades governamentais ou de caráter público" (Brasil, 2011).

Mais uma vez ressalta-se que isso é válido somente em caso de informações personalíssimas, ou seja, dados referentes ao próprio solicitante. Mendes (2014) menciona que quando se tratam de dados de terceiros, a situação se torna um pouco mais complexa. Isso porque, por um lado, há o dever de uma Administração Pública transparente, mas se diversas informações forem fornecidas desenfreadamente, a privacidade de muitos indivíduos, certamente, será violada.

Deve ser mantido, portanto, um equilíbrio, “o máximo de transparência possível, com a quantidade de sigilo necessário” (Bull *apud* Mendes, 2014, p. 151).

A LAI ainda traz em seu bojo a noção de informação pessoal: “art. 4º, IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável” (Brasil, 2011). Destaca-se também o art. 31 “o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais” (Brasil, 2018). Acabando, autores afirmam que, já nessas legislações mais antigas, é possível detectar um direito à proteção de dados (Mendes, 2014).

3.7 Marco Civil da Internet – Lei N° 12.965/14

O Marco Civil da Internet (MCI) vem com o objetivo de tornar a navegação, na rede de computadores, mais segura; para isso, estabelece direitos e deveres a serem cumpridos com o intuito de pôr fim à ideia de que, dentro da internet, absolutamente tudo é permitido.

No que se refere a proteção de dados, dentre as legislações até aqui citadas, o MCI é, sem dúvidas, a mais detalhada. Nas palavras se Oliveira (2018):

> O MCI e o Decreto são, de longe, as normas mais detalhadas que versam sobre a proteção de dados pessoais, estabelecendo, entre outras disposições, as definições legais essenciais para seu entendimento e aplicação, especialmente as de “dados pessoais” e de “tratamento”, a privacidade como um princípio do MCI e um direito dos usuários da Internet e padrões de segurança para guarda, armazenamento e tratamento de dados pessoais (Oliveira, 2018, *online*).

Contudo, ele é insuficiente, vez que, seu artigo 1º preceitua que essa legislação somente se aplica às relações jurídicas provenientes da internet: “esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria” (Brasil, 2014).

Depreende-se que o seu foco não é o tratamento de dados em si, mas sim a internet. Logo, com base no MCI, só é possível pensar em tratamento de dados se esse foi realizado ou dentro, ou com a participação da web (Oliveira, 2018).

Ainda, o art. 7º do MCI, assegura aos usuários o direito de (I) não fornecer seus dados a terceiros, salvo mediante consentimento livre, expresso e informado;

(II) consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (Brasil, 2014).

Pois bem, vale salientar que o presente capítulo limita-se a breves menções a respeito das legislações que, de algum modo, contribuíram para o ordenamento jurídico e antecederam a LGPD, grande marco normativo, que será matéria de outro capítulo.

4 CONCEITO DE PRIVACIDADE

Como dito anteriormente, a manifestação em solicitação à privacidade não é um acontecimento do mundo contemporâneo. Segundo Miranda (2013, p. 218) "[...] em toda fase da evolução humana o indivíduo sempre manifestou a necessidade de preservar alguns fatos e acontecimentos do conhecimento público".

Em um período onde não existia carta, telefone ou internet, a proteção da propriedade foi o meio encontrado para preservar a privacidade, mas essa proteção não era igualitária, já que o direito à propriedade era uma opção facultada somente à burguesia. Inclusive, isso pode ser bem observado no caso *Prince Albert vs*. *Strange*[2] (Miranda, 2013).

Posteriormente, a ideia de privacidade teria sofrido evolução através dos pensamentos liberais do filósofo Stuart Mill. Nesse momento a privacidade era vista como aspectos concernentes à vida do indivíduo, como ideologias e escolhas de pensamento, mas não era tida ainda como direito autônomo (Miranda, 2013).

Surgindo, depois, o *Right to Privacy*, já mencionado neste instrumento. Mendes (2014, p. 28) explica que o artigo é importante por conta das delimitações feitas pelos autores, deste modo:

> (a) o direito à privacidade não impede a publicação do que é de interesse geral;
> (b) o direito à privacidade não veda a comunicação de tudo que é privado, pois se isso acontecer sob a guarda da lei, como, por exemplo, em um Tribunal ou em uma Assembleia Legislativa, não há violação desse direito;
> (c) a reparação não será exigível se a intromissão for gerada por uma revelação verbal que não cause danos;
> (d) o consentimento do afetado exclui a violação do direito;
> (e) a alegação de veracidade da informação pelo agressor não exclui a violação do direito;
> (f) a ausência de dolo também não exclui a violação desse direito (Mendes, 2014, p. 28).

Além disso, através do artigo os autores manifestam pela insuficiência do direito de propriedade como forma de proteger a privacidade dos indivíduos (Dalese; Palmeira, 2023, *online*). Cabe ressaltar que nesse momento a privacidade ainda possuía caráter individualista, assemelhando-se aos direitos de primeira dimensão ou geração, que exigiam uma abstenção do Estado na esfera individual (Mendes,

[2] ***Prince Albert vs. Strange*:** trata-se de um episódio em que a Família Real obteve uma *injuncton* reconhecendo o direito de propriedade sobre telas ilustradas com figuras íntimas de seus membros, impedindo, portanto, a posterior exibição de tais gravuras (Miranda, 2013, p. 219).

2014). Em concordância, Cueva (2016, *online*) informa que o direito à privacidade só foi reconhecido como direito coletivo ou difuso, em 1983.

Ante o exposto, é possível concluir:

> [...] verifica-se que a dimensão do conteúdo do direito à privacidade parte de uma compreensão burguesa, como argumento hábil para defesa da propriedade, e evolui até o reconhecimento de um direito próprio, dotado de autonomia, tendente a tutelar os pensamentos, as emoções e as sensações dos indivíduos, ou seja, aspectos ligados à vida privada e a intimidade do ser humano (Miranda, 2013, p. 221).

Miranda (2013) explica que conceituar ou delimitar o termo privacidade parece ser uma atividade difícil, já que quase não existem conceitos fechados a respeito do tema nas doutrinas disponíveis. Embora esse termo venha sendo debatido desde o século XIX, até hoje ele não foi precisamente conceituado. Os conceitos presentes nas legislações e jurisprudência apenas se preocupam em identificar e tipificar as violações e ameaças, não tentando estabelecer conceitos. “As numerosas definições legais, assim como o conjunto de decisões jurisprudenciais que tutelam este direito, não contém uma definição precisa do conteúdo do direito à privacidade” (Miranda, 2013, p. 221).

Mas, há controversas, Ferraz Jr. (1993, p. 1), por exemplo, afirma que privacidade pode ser definida como: “[...] o direito de o indivíduo excluir do conhecimento de terceiros aquilo que a ele só é pertinente e que diz respeito ao seu modo de ser exclusivo no âmbito de sua vida privada”.

Em sua obra, Miranda (2013, p. 224) chega a fazer referência ao termo de Ferraz Jr.:

> [...] a privacidade consiste em direito subjetivo fundamental, cujo titular é toda pessoa, física ou jurídica, brasileira ou estrangeira, residente ou em trânsito no país, cujo conteúdo é a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por só a ele lhe dizerem respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão, ou seja, integridade moral do titular. (Ferraz Jr. *apud* Miranda, 2013, p. 224).

Para terminar, constata-se que “[...] conceituar privacidade implica falar sobre sentimentos, ações e abstenções, que podem ser altamente meritórios do ponto de vista da pessoa a que se referem, mas que, vistos do exterior, tendem a apoucar a ideia que deles faz o público em geral”. (Miranda, 2013, p. 225).

4.1 A Proteção de Dados Como Direito Fundamental

Em concordância com o que foi exposto em capítulos anteriores, o direito à privacidade vem sendo tratado, em instrumentos, desde a Declaração Universal dos Direitos Humanos. Pouco a pouco, esse direito foi introduzido em legislações dos mais diversos países, cada um à sua maneira.

No Brasil, a Constituição Federal, em seu artigo 5°, prevê expressamente vários direitos relacionados à privacidade e informação, no Título II - dos direitos e garantias fundamentais:

> Artigo 5º: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
> V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;
> [...]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
> [...]
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional (Brasil, 1988).

Doneda (2008) afirma que os direitos consagrados nesses incisos são generalistas e abstratos. Segundo ele, o legislador etiquetou, com proibições e permissões, o uso das informações em um sistema que causa ambiguidade, e essa ambivalência só poderia ser desfeita através de várias análises, do contexto em que as informações foram coletadas, da finalidade e do âmbito em que será tratada.

> Tal técnica legislativa acabou por fundamentar uma interpretação temerosa no que no que diz respeito à matéria: se, por um lado, a privacidade é considerada um direito fundamental, as informações pessoais em si parecem, a uma parcela substanciosa da doutrina, estar protegidas somente no que se refere à sua “comunicação”, como pode sugerir o art. 5° [...] Este hiato segrega a tutela da privacidade [...] e possibilita uma perigosa interpretação que pode eximir o aplicador de levar em conta os casos nos quais uma pessoa é ofendida em sua privacidade – ou outros direitos fundamentais – não de forma direta, porém pela utilização abusiva de suas informações pessoais em bancos de dados (Doneda, 2008, p. 31).

Já outros autores, como Fortes e Boff (2014, p. 119), alegam que o texto constitucional é bem completo no que tange a proteção da privacidade, mas ainda assim, há necessidade de diversas discussões a respeito do tema, pois esse único texto não é capaz de atender muitíssimas novas demandas.

Corrobora Mendes (2014), quando explica que esses artigos devem ser observados como algo incompleto e passíveis de mutações, mesmo porque “a vitalidade e a continuidade da Constituição dependem da sua capacidade de se adaptar às novas transformações sociais e históricas, possibilitando uma proteção dos cidadãos contra novas formas de poder que surgem na sociedade”. (Mendes, 2014, p. 169).

Em vista disso, algo importante deve ser observado: se de um lado a Constituição deve idealizar a noção de permanência e estabilidade, de outro, ela deve sempre ser capaz de expressar atualização através da abertura de interpretação com o fim de fazer valer os princípios nela consagrados (Mendes, 2014).

Antes mesmo da LGPD, por meio de sua obra, Mendes (2014) deixa claro que através de análises jurisprudenciais é possível concluir que a proteção de dados foi incorporada ao ordenamento jurídico brasileiro. Isso porque, não há sentido em excluir a proteção de dados da interpretação do texto constitucional, vez que, o tratamento de dados, naquela época (2014), já era considerado uma ameaça muito maior do que os perigos costumeiros, quais sejam: jornais e paparazzis. Ela completa:

> [...] se não há dúvidas de que a Constituição Federal protege o homem médio desses riscos, que raramente ocorrem na vida real, não haveria sentido em negar-lhe a proteção constitucional perante os bancos de dados, que constituem um risco constante e diário para todos os cidadãos (Mendes, 2014, p. 171).

Além da análise jurisprudencial, somente examinado em conjunto o artigo 5º da Carta Magna, a garantia do *habeas data* e o princípio fundamental da dignidade humana, é possível concluir que está presente na Constituição o direito fundamental à proteção de dados pessoais (Mendes, 2014).

Por fim, conclui-se que a proteção de dados como direito fundamental não é mera possibilidade, mais do que isso, “[...] trata-se de uma necessidade para tornar efetivos os fundamentos e princípios do Estado Democrático de Direito, na

sociedade contemporânea da informação, conforme determina a Constituição Federal" (Mendes, 2014, p. 172).

4.2 O Valor dos Dados Pessoais

Hoje, vive-se a era da economia dirigida por dados, onde esses são vistos como potenciais ativos pelas grandes e pequenas empresas e são essenciais para concretização dos negócios. Tornaram-se, mais do que nunca, uma espécie de insumo capaz de movimentar todos os setores da economia. Inegável, pois, que até a Administração Pública, em todos os seus níveis, se beneficia da economia movida pelos dados, já que eles tornam possível a concretização de políticas públicas e de diversos outras encargos (Ferraço, 2018).

Os dados estão presentes em todos os lugares, em todas as atividades. Eles não passam despercebidos, são coletados e armazenados em base de dados que crescem cada vez mais.

Infelizmente, o uso de aparelhos eletrônicos tem se tornado, a cada dia, mais frequente; normalizou-se o ato de acordar pela manhã e ter como objetivo imediato conferir o celular, verificar primeiramente o horário; depois, as notícias; o clima; somente com isso, os sistemas informatizados já possuem em suas bases uma gama de dados referentes ao cotidiano desse indivíduo. Quando sai de casa para ir ao trabalho, o celular, o relógio, ou o aplicativo presente na multimídia do carro traça e armazena o caminho feito com frequência e, em um outro dia qualquer, o usuário é surpreendido com uma sugestão de rota alternativa para se esquivar do trânsito. Em aplicativos de música, ou plataformas que oferecem filmes e séries, os gostos e preferências dos usuários são registrados e, dia após dia, aparecem novas sugestões de filmes e músicas. O aplicativo de mensagens registra suas ligações, talvez até o conteúdo. Já o do banco registra todas as transferência e transações. Enfim, "tudo é mensurável em dados, que podem revelar quem somos" (Ferraço, 2018, p. 6).

A partir do exposto, percebe-se uma exposição, quase que involuntária, dos seres humanos à tecnologia de uso diário, que parece inofensiva; mas, além dessa exposição forçada, tem-se também aquela feita por pura escolha do indivíduo. Heen (*apud* Boff; Fortes, 2014) define esse momento da história como "era do culto amador", onde pessoas são induzidas ao exibicionismo, e acabam por renunciar a

própria privacidade quando fornecem dados valiosos às grandes corporações, como *Google e Facebook.* Nota-se, então a figura do homem digitalizado, translúcido a ponto de exigir fortes normas para a proteção da sua vida privada, intimidade e liberdade (Silveira, 2023).

5 A LEI GERAL DE PROTEÇÃO DE DADOS

Não obstante algumas leis, já citadas anteriormente, protegerem de algum modo os direitos relacionados à privacidade de dados, a preocupação com o correto tratamento de dados se intensificou com o crescimento exponencial da tecnologia; aquela responsável por trazer à tona a era digital, relacionada com uma nova economia que depende, e muito, das bases de dados (Pinheiro, 2023). Logo, para outorgar mais segurança jurídica e tornar o Brasil mais competitivo a nível de proteção de dados, foi promulga em 2018 a Lei Geral de Proteção de Dados (LGPD), a qual reúne em um só diploma todas as legislações esparsas que trataram do tema, como por exemplo o CC, CDC, a Lei do Cadastro Positivo, o MCI, a Lei de Acesso à Informação Pública e a Lei do *Habeas Data* (Silveira, 2023).

A LGPD pode ser definida como:

> [...] um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas (Pinheiro, 2023, p. 9).

Seu principal objetivo é proteger os direitos fundamentais de liberdade e privacidade, assim como o livre desenvolvimento da personalidade da pessoa natural, utilizando-se, para isso, da boa-fé como princípio para todas as formas de tratamento (Pinheiro, 2023).

A proteção do direito à privacidade está relacionada ao livre desenvolvimento da personalidade e, havendo impossibilidade do exercício de isolamento de dados pessoais, o direito à privacidade será exercido através da autodeterminação informativa; um fundamento que diz respeito ao controle que o titular possui sob seus dados, o qual concretiza-se por meio do consentimento, direito ao acesso e retificação das informações (Silveira, 2023).

Ilustrando dessa forma, parece até que as legislações de proteção de dados vieram como recurso de salvação somente para as pessoas naturais, contudo, esse pensamento está equivocado. Essas normas protegem e beneficiam um todo e não somente os consumidores, isso porque um consumidor seguro tende a ter mais confiança ao realizar determinada operação, criando, assim, um cenário positivo para a economia dos diversos países inseridos nessa cadeia. “Um regime de

proteção de dados, quando eficaz e plenamente vigente, impulsiona o surgimento de ecossistema de dados, no qual todos os setores da sociedade, inclusive o cidadão, são diretamente beneficiados" (Ferraço, 2018, p. 4).

Pois, passa-se agora a análise dos pontos principais da legislação.

5.1 Dados Pessoais

"Na Lei Geral de Proteção de Dados, parte-se da ideia de que todo dado pessoal tem importância e valor". (Bioni *et al*., 2020, p. 131). Isso se faz necessário porque, muitas vezes, determinada informação, sobre determinada pessoa, não terá, em um primeiro momento, o condão de identifica-la, mas, se cruzada com outros dados, certamente uma pessoa específica tomará forma (Bioni *et al*., 2020).

Nota-se, então, um cuidado muito grande com os dados, isso fica explícito já no primeiro artigo, onde se menciona que toda pessoa que trate de dados, seja ela natural ou jurídica, deve se submeter ao crivo dessa legislação.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

No art. 2º tem-se os fundamentos da norma que, segundo Silveira (2023) vão além do interesse individual do ser e alcançam aspectos concernentes ao direito empresarial e econômico, pois além de prever expressamente os direitos relativos à personalidade do indivíduo, prevê também como fundamento o direito à livre iniciativa, livre concorrência, desenvolvimento econômico, tecnológico e inovação. O autor explica ainda que isso se dá porque o uso de dados como produto motiva concorrência no mercado, daí a necessidade de positivação.

Outrossim, a lei é aplicável ao tratamento de dados em âmbito físico ou digital, e pode ocorrer dentro ou fora do país, além disso, protege também o estrangeiro em trânsito no Brasil.

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei (Brasil, 2018).

Como dito, observa-se com a leitura do artigo que essa legislação possui efeitos extraterritoriais, ou seja, internacionais, pois, se a coleta for realizada dentro do território brasileiro, e os dados, posteriormente, forem tratados fora do Brasil, a LGPD deverá ser observada (Garrido, 2023).

De outro modo ocorre no artigo 4º, onde está explícito que a lei não é aplicável quando o tratamento de dados for realizado por uma pessoa natural, desde que os fins sejam exclusivamente particulares e não econômicos. Igualmente não se aplica quando houver finalidade exclusivamente jornalística ou artística, bem como quando utilizada para fins de segurança pública ou defesa nacional (Garrido, 2023).

No artigo 5º é possível perceber que essa legislação adota o sentido amplo relativamente ao conceito de dados pessoais:

> Art. 5º Para os fins desta Lei considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> [...]
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; (Brasil, 2018).

O conceito amplo de dados pessoais é reforçado, segundo Silveira (2023), pelo inciso XI, do mesmo artigo, que prevê a desvinculação entre dado e titular, e nessa hipótese, não há alcance da tutela da LGPD, pois, essa só terá incidência se o dado apresentar potencial identificação com alguma pessoa. Ainda, percebe-se que os dados são divididos em dados pessoais e dados pessoais sensíveis, e esse segundo merece atenção redobrada do controlador. Por último, o art. 12, § 2º menciona: “poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada” (Brasil, 2018). Esses dados vão além dos sensíveis, são referentes à opinião, declarações ou comportamentos utilizados no meio virtual. Portanto, nítido mais uma vez o caráter amplo de conceito de dados,

onde qualquer informação identificada ou identificável e relacionada à pessoa certa é objeto de proteção da LGPD (Silveira, 2023).

5.2 Consentimento

O consentimento é a base para o tratamento de dados do titular pelo controlador, é através dele que o titular exerce a autodeterminação informativa; ele pode ou não autorizar o tratamento de seus dados e, se a resposta for negativa, o controlador fica totalmente impedido de realizar o tratamento. Contudo, se autorizado, o consentimento fica adstrito a finalidade informada pelo controlador (Brasil, 2019).

A respeito do consentimento, importante mencionar que algumas empresas condicionam o direito ao fornecimento de um serviço à entrega de informações, inclusive, a LGPD não proíbe tal fato, ela somente exige que, nesses casos, o titular seja manifestamente informado sobre esse fato, bem como aos meios pelo qual ele poderá exercer os seus direitos de titular. A respeito disso, Silveira (2023) informa que essa prática, além de estar em desacordo com o artigo 39 do CDC, viola o fundamento da autodeterminação informativa porque impede o controle do titular sobre os dados que ele realmente deseja informar. Ele completa:

> Nesses casos de imposição de condicionantes, o titular não consente de forma livre, embora informada ou inequívoca quanto à determinada finalidade. A informação quanto à finalidade, quando imposta condição, afeta a liberdade e o controle que o titular exerce sobre seus dados (Silveira, 2023, *online*).

Ainda sobre o consentimento, quando se fala de tratamento de dados, o inconveniente não se limita a um possível dano causado pelo seu vazamento, com consequente acesso de terceiros não autorizados. Mais importante do que isso é a perfeita simetria entre a seleção de informações alinhada à finalidade do consentimento. Isso porque se os gigantes do meio tecnológico, como *Facebook, Google, Amazon* e *Microsoft*, que têm a sua disposição bilhões de dados, de diversos tipos, sobre várias pessoas diferentes, decidirem utilizar de tais informações para finalidade alheia aquela originalmente concedida, certamente poderão influenciar a seu próprio benefício – ou, de quem estiver disposto a pagar - uma multidão de pessoas. Assim como já ocorreu no caso *Cambridge Analytics* (Silveira, 2023).

Desse modo, a maior garantia que a pessoa natural pode obter em relação aos seus dados, é de que o consentimento estará sempre associado à finalidade pela qual foi solicitada.

5.3 Titulares e Destinatários na LGPD

Como bem dito, a Lei Geral de Proteção de Dados tutela a privacidade e liberdade da pessoa natural, a qual é considerada como primeiro interesse do ordenamento jurídico. Assim, o titular da norma referida é a pessoa natural cujos direitos fundamentais precisam ser resguardados (Silveira, 2023).

Logo, por se tratar de um direito fundamental, a tutela oferecida pela LGPD, não se limita a proteção somente dos que aqui residem, estende-se também aos estrangeiros, desde que os dados sejam tratados em território nacional (Brasil, 2018). Nesses termos, sendo pessoa natural, integra a posição de titular na relação jurídica causada pelo diploma de proteção de dados, e assim tem o condão de exigir o cumprimento da lei (Silveira, 2023).

Com base nisso, cabe fazer uma ponderação: embora não expresso em nenhum de seus artigos, a proteção prevista na LGPD não atinge as pessoas jurídicas (Oliveira, 2018). É bem verdade que a pessoa jurídica é suscetível de direitos e obrigações, assim como as pessoas naturais, essa, entretanto, é a única similaridade entre elas. Ao contrário das pessoas jurídicas, a pessoa natural não nasce plenamente desenvolvida, e para se desenvolver, ela precisa do direito de ser deixada só; dessa forma, a privacidade é essencial para a construção do ser humano. Já as pessoas jurídicas não possuem a mesma necessidade, pois são meras ficções, capazes apenas de emprestar da pessoa natural a consciência que necessitam para a realização de suas atividades. Logo, segundo o autor Ricardo Alexandre de Oliveira (2018), não há o que ser discutido, a preservação da privacidade é útil somente para o ser humano.

Silveira (2023) discorda, apesar de reconhecer a diferença existente entre as pessoas naturais e jurídicas, ele aduz:

> Não são estranhas as proteções de sigilo que a lei outorga às pessoas jurídicas em relação aos livros mercantis, livros contábeis, segredo industrial e patentes, por exemplo. Essa proteção direciona-se à pessoa jurídica em relação à atividade por ela realizada. Nada mais coerente que estender às pessoas jurídicas a proteção de dados de que são titulares quando

> ocuparem posições jurídicas idênticas às tituladas pela pessoa natural. Não obstante, o tema não é fácil e necessita de maior sedimentação.

Agora, no que se refere aos destinatários, observa-se o contrário, esses independentemente de serem pessoas naturais ou jurídicas – de direito privado e público - devem obediência à LGPD pois integram um dos polos da relação jurídica de direito material prevista por essa legislação (Brasil, 2018). Há, entretanto, ressalvas, previstas no art. 4º da LGPD, ficam excepcionados da incidência dessa obediência; para que o presente instrumento não se estenda demasiadamente, tais exceções não serão comentadas uma a uma.

Pois bem. Os destinatários são divididos em três grupos: "(i) as pessoas naturais que tratam dados do titular; (ii) as sociedades empresárias e simples; e (iii) a Administração Pública em geral". (Silveira, 2023, *online*). Portanto, dada as várias obrigações impostas pela lei, exige-se desses destinatários - também chamados de controladores - grandes condutas, comportamentos e deveres que almejam o correto tratamento de dados do titular e podem ser observados no art. 5º, mas abaixo apresentam-se de maneira sintetizada:

> [...] deveres de conduta, de observância à regra, de imposição de comportamento para gerenciamento dos riscos dos processos de tratamento de dados da pessoa natural e dos procedimentos previstos para evitar ou mitigar o risco de ocorrência de dano consistente na violação das normas da LGPD e, em específico, dos riscos de violação aos direitos individuais fundamentais da pessoa humana pela desconformidade do tratamento de dados pelo controlador. (Silveira, 2023, *online*).

Aqui, importante mencionar os termos trazidos por essa legislação: (I) controlador é aquele responsável pelas decisões referentes ao tratamento de dados pessoais (art. 5º, VI); (II) operador é aquele que realiza o tratamento de dados pessoais a mando do controlador (art. 5º, VII) – ambos são definidos também como agentes de tratamento; (III) encarregado é aquele designado pelo agente de tratamento com a finalidade de realizar a comunicabilidade entre o controlador, o titular e a ANPD (Brasil, 2018).

A fim de finalizar, acrescenta-se a ideia de que além de fazer o possível para a correto cumprimento da legislação, por meio de programas, gestão de riscos, bem como mitigar eventuais danos, cabe também aos destinatários "obstar qualquer exigência de exercício de direitos do titular em relação ao tratamento de seus dados que não estejam contemplados na norma ou que extravasem o necessário à sua proteção" (Silveira, 2023, *online*).

5.4 Princípios da LGPD

Os princípios são regras-mestras do ordenamento jurídico. Paulo Barros de Carvalho (*apud* Oliveira, 2018) explica:

> Princípios são linhas diretivas que informam e iluminam a compreensão de segmentos normativos, imprimindo-lhes um caráter de unidade relativa e servindo de fator de agregação num dado feixe de normas. Exerce o princípio uma reação centrípeta, atraindo em torno de si regras jurídicas que caem sob seu raio de influência e manifestam a força de sua presença. (Carvalho *apud* Oliveira, 2018, *online*).

Dito isso, a LGPD possui dez princípios, que estão previsto no artigo 6º; a intenção deles é "fazer com que a lei se torne referência à produção legislativa posterior, bem como para a interpretação de outras normas que tenham como tema o tratamento de dados pessoais". (Oliveira, 2018, *online*). Em razão disso, o interessado em tratar de dados pessoais, em especial as empresas que lidam diariamente com a coleta de dados, precisam observar, compreender e implementar de forma rigorosa tais princípios (Santos; Taliba, 2018).

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Brasil, 2018).

Nota-se que os princípios devem ser observados sob a ótica da boa-fé, pois ele guiará o comportamento das empresas que coletam e tratam os dados pessoais (Santos; Taliba, 2018). Além disso, o princípio da finalidade e da necessidade são considerados, na visão de Ricardo Alexandre Oliveira (2018), as pedras de toque na metodologia da LGPD, porque repercutem seus efeitos em outros dispositivos.

A respeito da adequação, presente no inciso II, ressalta-se que mesmo quando houver dispensa da necessidade do consentimento, as informações deverão ser utilizadas, só e somente só, para a finalidade pelas quais foram colhidas e cientificadas ao titular. Assim, as autoras Fabíola e Rita ensinam:

> [...] se um passageiro informa à empresa aérea sua restrição alimentar, o faz para que possa receber alimentação específica no voo, e não para que sejam vendidos seus dados para empresa alimentícia que passará, com base nisso, a lhe ofertar alimentos compatíveis com sua restrição alimentar. (Santos; Taliba, 2018, *online*).

No inciso III, é possível perceber a ideia de uma prática de minimização de dados, segundo a qual, para o fornecimento de um serviço ou produto, somente os dados estritamente necessários deverão ser coletados. Isso se aplica, inclusive, às autoridades, ainda que essas não precisem observar o consentimento dos titulares. Portanto, no momento da coleta, o operador deve se questionar se há mesmo necessidade de colher tal dado, e inexistindo, não deverá coleta-lo sob pena de ser abusivo (Santos; Taliba, 2018). Concorda Carolina Peck Garrido (2023) quando ensina que a ideia básica no tratamento de dados pessoais parte do consentimento do titular, que quando exigido, deve ser inequívoco; bem como, precisa estar associado às finalidades apresentadas.

Além do consentimento inequívoco e da ciência da finalidade, o titular também deve ter acesso ao tipo de tratamento, e em caso haja divulgação, há obrigação de informar a quem os dados serão transmitidos. O dono dos dados pode solicitar sua retificação ou revogar o consentimento, inclusive, exigindo sua exclusão (Santos; Taliba, 2018).

Levando em consideração, ainda, todo o amparo que a LGPD oferece ao titular, o consentimento pode ser declarado nulo quando as informações oferecidas ao proprietário forem enganosas, abusivas ou não forem comunicadas com clareza e sem ambiguidades. E de acordo com o princípio da finalidade, qualquer alteração na finalidade deve ser comunicada ao titular que terá a opção de concordar ou não

com a nova função, caso contrário, haverá violação da autodeterminação informativa (Santos; Taliba, 2018).

Pois bem, percebe-se aqui a improtelável necessidade de adequação por parte de todos aqueles que praticam a coleta de informações pessoais, tem-se um novo marco que traz consigo uma nova meta - colocar em prática todos esses princípios.

6 CONCEITO DE *COMPLIANCE*

O termo *compliance* tem origem no verbo inglês *"to comply",* que pode ser compreendido como "cumprir", "estar de acordo" ou "em conformidade". Trata-se de um programa corporativo que visa adequar uma empresa, por exemplo, à lei, norma de conduta interna ou algo semelhante (Scandelari, 2022). Os programas de *compliance* têm "a finalidade preventiva e mitigatória da ocorrência de danos consistentes na violação normativa, mediante análise de riscos, ao promover cultura de ética no ambiente empresarial". (Silveira, 2023, *online*).

Segundo Marco Antônio Karam Silveira (2023), o termo *compliance* pode ser repartido em dois enfoques, o amplo e o estrito. Em sentido amplo, o compliance trata da concretização de valores éticos e, para isso, vale-se de uma série de mecanismos preventivos e mitigadores estabelecidos de acordo com a atividade empresarial desempenhada pela empresa. Já no sentido estrito, *compliance* significa apenas observância às regras. Ele ainda explica:

> O caráter interno do *compliance* denota sentido de autorregulação do comportamento que deve ser observado pelos integrantes de uma certa e determinada organização privada ou pública em relação à atuação externa dessa organização. O agir externo do ente público ou privado é pautado internamente por regramento elaborado e incidente sobre os agentes que o elaboram, por isso, autorregulação. O agir em conformidade com a norma (regra ou princípio), função original e restrita do programa de conformidade, desdobra-se, pela própria evidência da obrigatoriedade em observar a norma e em não a violar, em deveres de comportamento ético interno para além do texto normativo, que se projetam na atuação externa do ente que o elabora e o segue. (Silveira, 2023, *online*).

Dessa forma, o compliance tem o condão de prevenir e reparar infrações, de forma distinta da função exercida pela responsabilidade civil, vez que essa segunda geralmente é invocada após o efetivo dano causado pela empresa, mediante imposição judicial, a fim de majorar eventual verba indenizatória e desestimular a produção de outros danos (Silveira, 2023).

Aqui cabe distinguir também o *compliance* das práticas de governança corporativa. Silveira (2023, *online*) ensina que enquanto a governança deve ser observada "de forma restrita ao ambiente interno das corporações, imediatamente, envolvendo sócios, administradores, órgãos e funções de comando da companhia", o *compliance* estabelece regras para todos os colaboradores, principalmente para os funcionários e prestadores de serviço e não apenas para sócios e administradores. Não obstante a diferença citada, esses termos apresentam alguma relação, pois os

programas de compliance são também definidos como “instrumentos de governança corporativa tendentes a garantir que as políticas públicas sejam implantadas com maior eficiência”. (Cueva *apud* Silveira, 2023).

Pois bem. É uma ferramenta que tem por objetivo implementar missões e valores dentro de determinada empresa ou organização e, para isso, é essencial que a empresa adote um comportamento focado na redução de riscos à própria empresa (Moussallem; Rocha; Wervloet, 2020).

> Os principais objetivos da implementação de um programa de *compliance* são o cumprimento da legislação nacional e internacional, além das normas internas que regem a empresa, prevenir demandas judiciais e obter transparência na condução dos negócios, sendo figura essencial à boa governança corporativa e desenvolvimento transparente e sustentável na gestão, fundamentais à função social da propriedade. (Moussallem; Rocha; Wervloet, 2020, *online*).

Logo, através do compliance, as organizações conseguem identificar e gerenciar melhor os riscos decorrentes da violação de uma legislação ou de sua conduta interna e, a longo prazo, uma espécie de “cultura” será enraizada na corporação. Isso, por sua vez, aumenta a eficiência e o valor da empresa no mercado, e faz com que a mesma tenha acesso a recursos. Ressalta-se ainda, que os programas podem ser adaptados conforme os diversos ramos de atividades, de acordo com a jurisdição ou o nível de risco. (Moussallem; Rocha; Wervloet, 2020). Por fim, o programa de compliance é capaz também de atenuar determinada penalidade imposta por autoridade (Silveira, 2023).

6.1 Origem Histórica

Por obvio, assim como o termo compliance decorre de um verbo no estrangeiro, sua origem também teve início no estrangeiro. A ideia de implementação e registros do comportamento de determinada corporação se deu, inicialmente, pela exigência de observância da lei de combate a corrupção, conhecida como *Foreign Corrupt Practices Act* (FCPA), nos Estados Unidos em 1977 (Silveira, 2023).

Já no Brasil, esse programa ganhou força a partir de 2013, em decorrência também de uma lei de combate a corrupção - Lei Anticorrupção (12.846/13) - que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeria - isso porque,

após *vacatio legis*, a Lei Anticorrupção passou a exigir critérios mínimos para a contratação de sociedades empresárias, gerando então a necessidade de adequação por parte das empresas, a fim de evitar eventuais sanções (Moura e Souza, 2022).

6.2 Programas de *Compliance* Para Observância da LGPD

Como mencionado, se não cumprida corretamente, a Lei Geral de Proteção de Dados prevê penalidades que podem gerar grandes encargos para as empresas, sejam eles financeiros ou relativos à reputação. Para que isso não ocorra, um programa de conformidade é mais que bem-vindo, pois ele tornará possível a observância da legislação por completo.

Segundo Silveira (2023), o art. 5º, inc. XVII, da LGPD sugere fortemente a necessidade de implementação de um programa de conformidade quando exige um relatório de impacto à proteção de dados pessoais, o qual trata-se um documento contendo os riscos às liberdades civis e direitos fundamentais, assim como medidas capazes de mitigar tais prejuízos.

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (Brasil, 2018).

Existem ainda outros dispositivos que afirmam a pertinência dos programas de *compliance* a fim de alcançar a plena aplicabilidade da tutela de dados, como por exemplo o art. 41, inciso III; art. 46, *caput;* art. 48, *caput*; art. 49; art. 50, *caput*, §§ 1º e 2º, inciso I, alíneas “a” a “h”, inciso II, e § 3º; e art. 52, § 1º, incisos VIII, IX e X. Ressalta-se que desses dispositivos citados, os mais pertinentes, serão objeto do próximo capítulo.

Por enquanto, cabe deixar claro que o primeiro requisito a ser observado por um programa de conformidade ou de *compliance* é a regra do consentimento do titular. Uma vez presente, os agentes de tratamento estarão legitimados e a preocupação passa a centrar-se nos riscos e dimensão do tratamento, bem como no estabelecimento de condutas e rotinas para o cumprimento da legislação (Silveira, 2023).

Para que o compliance seja efetivo, o consentimento deve ser observado até na fase pré-contratual (Silveira, 2023). O art. 8 da LGPD prevê que para o consentimento ser válido, é necessária a manifestação do titular, que pode ser por escrito – em cláusula destacada - ou de outro modo, logo não se exige muitas formalidades (Brasil, 2018). O mesmo não ocorre em relação aos dados sensíveis, que exige sim formalidade como requisito para o tratamento (Brasil, 2018).

Destaca-se que o ônus da prova a fim de demonstrar que houve consentimento cabe ao controlador (Brasil, 2018).

Além da manifestação do titular, o consentimento, para ser válido, precisa ser informado. Isso significa que ele deve ser precedido de uma lista de informações que dizem respeito à finalidade, duração do tratamento, informações do controlador, uso e compartilhamento, direitos do titular e responsabilidade doa gente. Se ausente um item, o consentimento será nulo (Silveira, 2023).

No que tange a finalidade, necessário destacar que a falta de formalidades não permite que a finalidade do consentimento seja desviada, tampouco genérica. Outrossim, a finalidade é considerada uma extensão do consentimento; e se, em alguma hipótese, não for possível aferir a finalidade, a LGPD recomenda que seja feita uma ponderação entre a adequação e a necedade (Brasil, 2018).

6.3 Impactos dos Programas de *Compliance* na LGPD

A data limite para a adequação das empresas à LGPD terminou em 31 de julho de 2021, e as empresas que não se adequarem ou falharem nas regras podem ser punidas com multas milionárias, além de possível responsabilização civil e penal.

A empresa, para se adequar, não deve apenas seguir à risca o que está previsto na legislação, mas sim estabelecer uma nova mentalidade ou cultura que deve ser colocada em prática desde o momento da possibilidade de oferta de um serviço, por exemplo. “[...] o artigo da LGPD prevê adoção de medidas para proteção dos dados pessoais desde a “concepção” do produto ou serviço”. (Santos; Taliba, 2018, *online*).

Assim, qualquer empresa, com estabelecimento no Brasil ou que coletem dados de pessoas localizadas no Brasil, deve adotar todos os princípios anteriormente mencionados, e isso tem de ser tido como meta, desde a criação do

sistema para coleta, e em todo momento posterior, e não somente quando os dados forem acessados ou transmitidos, por exemplo (Santos; Taliba, 2018, *online*).

Segundo a LGPD, o agente de tratamento deve observar todas as medidas de segurança, técnicas e administrativas que objetivam proteger os dados de possíveis acidentes, ilícitos ou não (Santos; Taliba, 2018, *online*). Aqui estão algumas das medidas a serem observadas:

a. relatório de impacto: a Autoridade Nacional de Proteção de Dados (ANPD) poderá designar ao controlador a execução de um relatório de impacto, que é definido, segundo o artigo 5º, XVII, como documentação "[...] que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (Brasil, 2018). Nas palavras das autoras Rita e Fabíola:

> [...] o relatório de impacto é a documentação que contém todo o ciclo de vida dos dados tratados, os procedimentos e riscos envolvidos, e as medidas que visam mitigar os riscos e/ou remediar os incidentes, e poderá ser obrigatório a depender do volume ou natureza dos dados tratados. (Santos; Taliba, 2018, *online*).

b. comunicação à ANPD e titulares: segundo a lei, o controlador é obrigado a comunicar à autoridade nacional e os titulares em caso de qualquer inconveniente que cause risco ou dano ao proprietário dos dados. Segundo a ANPD, a comunicação tem de ser realizada em até dois dias úteis a contar da ciência, e a autoridade competente pode estipular que seja realizada uma ampla divulgação do ocorrido, bem como impor medidas a fim de reduzir possíveis impactos. Assim, apesar da empresa se tornar descredibilizada no mercado, certamente se empenhará ao implementar medidas preventivas com a finalidade de resguardar os indivíduos cujos dados estão sendo tratados (Santos; Taliba, 2018).

c. estruturação de sistemas a fim de atender aos requisitos de segurança, boas práticas e governança: segundo o artigo 46 da LGPD, os sistemas empregados para manusear dados devem ser formados de forma a atender os padrões de segurança, os de boas práticas e governança, bem como os princípios (Brasil, 2018). Nesse diapasão:

> A Autoridade Nacional de Proteção de Dados poderá dispor sobre padrões técnicos mínimos, considerando a natureza das informações tratadas (lembrando-se que os dados sensíveis requerem proteção maior), as características do tratamento e o estado da arte, e o controlador deverá garantir a proteção de dados mesmo após o término do tratamento (Santos; Taliba, 2018, *online*).

Outrossim, tanto os controladores, como os operadores, poderão, individualmente ou através de associações, desenvolver regras de boa conduta, ou até mesmo criar programas de governança, desde que observados alguns requisitos, é o que consta no art. 50:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (Brasil, 2018).

A LGPD prevê ainda que tais regras devem ser recicladas de tempos em tempos; esse período não é determinado pela lei, contudo os especialistas aconselham uma revisão, no mínimo quadrimestral (Santos; Taliba, 2018).

d. organização capaz de atender os princípios gerais da LGPD: a lei, em seu art. 49, prevê que os sistemas informatizados utilizados para o tratamento de dados devem ser montados para atender os requisitos de segurança e os princípios gerais. Dessa forma, as empresas tem necessidade de adaptar as equipes presentes na empresa, de forma que todas estejam alinhadas com o objetivo de alcançar a máxima eficiência no correto tratamento de dados. Ou seja, as áreas de *marketing*, tecnologia, jurídico, recursos humanos, logística, todas devem se pautar no *compliance* associado à proteção de dados (Santos; Taliba, 2018).

Enfim, se adotadas, essas medidas podem evitar cenários negativos, agregando confiabilidade às empresas e livrando-as de eventuais sanções ou responsabilizações. Nesse ponto, cabe transcrever aqui esse importante aprendizado:

> Ainda, importante destacar que um efetivo e bem elaborado programa de governança em privacidade, além de diferencial competitivo, auxiliará no ônus da prova que recai sobre o controlador quanto à obtenção do consentimento em conformidade com a lei, bem como nas hipóteses em que o juiz entender pela inversão do ônus, como quando a produção de prova pelo titular dos dados lhe resultar excessivamente onerosa (Santos; Taliba, 2018, *online*).

Contudo, se a relação entre a empresa e o usuário for pautada no consumo, sabe-se que a responsabilidade será objetiva, mas isso não interfere na relevância da governança, pois essa também serve para apuração de responsabilidades. Então se através da governança, os agentes de tratamento podem constatar e provar: (I) que não realizaram o tratamento lhe imputado; (II) que realizou o tratamento, mas

esse não violou a legislação de proteção de dados; ou (III) que o dano foi culpa exclusiva do titular ou de terceiros.

6.4 Pilares do *Compliance*

Como bem exposto, o *compliance* deve ser capaz de identificar e prevenir riscos causados pela violação de normas, bem como prever medidas capazes de tornar mais suave os danos causados; para que a vantagem desse programa seja maior e mais eficaz, alguns elementos precisam ser observados. Esses elementos são nomeados, pela doutrina, como pilares e serão aqui expostos de acordo com a ótica da LGPD, ou seja, de acordo com o contexto desse instrumento.

O primeiro deles denomina-se suporte da alta administração. Os detentores dos maiores cargos da empresa devem conceder o seu aval e apoio para que o *compliance* funcione. É necessário também que um profissional seja nomeado como responsável pela área do *compliance*; por obvio, essa pessoa necessita de competência suficiente para garantir a eficácia do programa, também precisa saber dialogar e influenciar positivamente os integrantes da equipe (Faria; Serpa; Sibille, 2020?).

Em segundo lugar, tem-se a avaliação periódica de riscos e manutenção do programa. Essa avaliação deve levar em consideração os riscos aos quais a empresa está submetida, que mudam a depender da área de atuação, dimensão e particularidades. Assim, se torna mais fácil projetar um programa personalizado, que realmente atenda as necessidades da organização. A legislação de proteção de dados é muito ampla – são vários as formas de tratamento de dados, em diversos níveis - assim como existem vários tipos de empresa, portanto, torna-se fundamental realizar uma avaliação personalizada (Reis, 2020).

Em terceiro lugar, tem-se a elaboração de códigos de ética e de conduta. Depois de identificar os riscos e a legislação a qual pretende se adequar, é necessário reunir esse conteúdo em uma documentação contendo as políticas que serão colocadas em prática pela empresa (Reis, 2020). Em seu artigo 50, inciso II, a LGPD incentiva tal prática a fim de tornar real o cumprimento das disposições (Brasil, 2018).

O quarto elemento trata-se do comprometimento da alta administração. Aqueles detentores dos maiores cargos devem, além de conceder aval, se

comprometer a observar todas as regras, pois se assim não for, os colaboradores terão a impressão de que o programa de compliance serve apenas como fachada (Reis, 2020).

Em quinto lugar, tem-se a necessidade de autonomia do setor de *compliance*. Reis (2023) explica que para melhor desempenho, esse setor precisa ter independência, pois em alguns casos, ele deverá tomar decisões e nem sempre será possível consultar outas áreas. Portanto, seja em um escritório apartado, seja dentro da própria corporação, o setor de adequação deve ser dotado de poderes para decidir o que entende ser melhor para a organização.

Em sexto lugar, têm-se os treinamentos periódicos. Claramente a empresa precisará comunicar e reforçar diversas vezes tudo que os colaboradores precisam colocar em prática. Cada funcionário, independentemente do cargo, precisa entender que ele é peça fundamental para o sucesso do programa (Faria; Serpa; Sibille, 2020?).

O sétimo é a criação de uma cultura de proteção. Trata-se de uma forma de pensar que deve ser repassada a todos dentro da empresa, desde o mais alto cargo até a base. Todos precisam entender como se portar diante da coleta de informações, bem como, os impactos negativos do uso irregular de tais informações (Reis, 2020).

O oitavo, consiste na criação de canais de denúncia. Esses servem para que pessoas possam alertar a empresa em relação a possíveis violações ao código de conduta, ou condutas inadequadas tomadas por colaboradores. É recomendável que haja opção de realizar denúncia anônima para que funcionários tenham confiança em comunicar algum ato inadequado feito até mesmo por algum colega de trabalho, facilitando assim o conhecimento de ilícitos (Faria; Serpa; Sibille, 2020?).

Por fim, tem-se a apuração e punição de condutas contrárias ao programa. Essa etapa deve ser rápida, sob pena de tornar perdido todo o trabalho construído pelo programa (Reis, 2020).

Para finalizar, Reis (2020) explica que esses são requisitos mínimos que devem ser analisados em conjunto com os princípios da LGPD; ela ainda menciona três pilares a serem adotados juntos com os já mencionados: prevenção, detecção e correção.

A prevenção é tida como mais importante, a empresa deve desempenhar todos os esforços a seu favor, “evitando acessos não autorizados, bem como

situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (Reis, 2020, *online*). Isso porque, no compliance digital, é muito mais fácil evitar um dano, do que reduzir os danos decorrentes do vazamento de dados. Já a detecção se torna possível principalmente através dos canais de denúncia. E, por fim, a correção "refere-se à tolerância zero para desvios em relação aos valores e princípios éticos da instituição" (Reis, 2020, *online*); desse modo, qualquer falha deve ser corrigida imediatamente, caso contrário, o trabalho do programa de adequação será perdido.

6.5 Desafios Para a Efetividade dos Programas de *Compliance*

Um dos desafios encontrados pelo programa de conformidade concentra-se no custo desempenhado pela empresa. Silveira (2023) explica que esses custos devem ser comparados aos ônus da legislação a qual a empresa pretende se adequar. Ocorre que o próprio autor reconhece que essa ponderação é difícil, ainda mais em se tratando da LGPD, uma lei que "faz variar percentuais de multa ou previsão de parâmetros ou critérios não objetivos em razão da não observância à norma". (Silveira, 2023, *online*). Ele explica também que muitos dos benefícios do *compliance* nem se quer são mensuráveis, é o caso da boa reputação e possibilidade de ampliação da corporação.

Ainda há de se considerar que quanto maior a empresa, maiores são os custos da conformidade, até porque "uma pequena organização empresarial não necessita adotar mecanismos tão requintados quanto outra grande e complexa". (Silveira, 2023, *online*). A própria LGPD reconhece a distinção entre grandes e pequenas empresas:

> Art. 55-J. Compete à ANPD:
> [...]
> XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; [...] (Brasil, 2018).

Em segundo lugar, tem-se como desafio para o programa de compliance a implementação da cultura de dados dentro da organização, pois essa conscientização deve atingir além dos sócios e administradores, devendo impactar também os colaboradores, clientes e fornecedores. "Não há como falarmos em

mitigação de riscos quando não há nem ao menos a ciência de que as regras do jogo mudaram e, assim, os dados devam ser protegidos em uma organização e pela organização". (Caovilla; Dufloth; Pazine, 2019, *online*). Os autores explicam que a linguagem fornecida pela LGPD é demasiadamente técnica, por isso a organização deve adapta-la as necessidades de compreensão dos colaboradores. Para isso, informativos, panfletos e treinamentos regulares são indispensáveis.

> [...] deve-se ter em conta que a mudança cultural apenas será progressiva e eficaz se a alta administração da organização der o tom adequado ao tema. O "tom" vindo da alta administração deve ser materializado em metas, métricas e monitoramento de resultados. Se assim não for, dificilmente haverá transformação cultural bem-sucedida em um ambiente corporativo. (Caovilla; Dufloth; Pazine, 2019, online).

Por último, o uso avaliação periódica de riscos, que consiste em um mapeamento de dados feito pela empresa. Tal ação deverá ser realizada periodicamente, pois a partir dela que serão identificados os riscos, bem como os planos de mitigação. Ocorre que esse passo, análogo ao relatório de impacto previsto na LGPD, consiste em uma tarefa difícil de ser realizada, pois além de contar coma ajudada de todos os colaboradores, deve ser muito minuciosa (Caovilla; Dufloth; Pazine, 2019).

7 CONCLUSÃO

Através do presente estudo, foi possível verificar a magnitude dos problemas gerados pela tecnologia. Esses problemas trazidos pela evolução tecnológica geraram, para o Estado e juristas, uma circunstância de inquietude, já que as legislações brasileiras anteriores ao ano de 2018 eram limitadas e tutelavam a privacidade e a proteção de dados sem grande dinamismo, de forma incompleta.

Nesse sentido, o advento da Lei Geral de Proteção de Dados pode ser considerado como um respiro para o direito e para a sociedade, pois ela é capaz de responder diversas questões encontradas no mundo jurídico quando se trata de dados, e principalmente, é capaz de salvaguardar o titular, vulnerável em relação às grandes corporações que se beneficiam do mercado de dados.

É possível constatar que o *compliance* é o instituto adequado para nortear as empresas no direito digital, no que tange a proteção de dados e aos desafios trazidos pela LGPD. Entretanto, se não for bem implementado e executado, servirá apenas de fachada, trazendo mais prejuízos do que benefícios.

Desse modo, o estudo teve como principais pautas: os motivos que ensejaram a criação da LGPD; o histórico anterior à LGPD; a pertinência dos dados pessoais na sociedade contemporânea e a necessidade de adequação por parte das empresas, a fim de evitar sanções e, principalmente, promover a proteção do titular.

A matéria trazida pelo presente instrumento encontrou alguns limites que moram exatamente na contemporaneidade do tema. Não obstante o longo histórico da proteção da privacidade, o cenário encontrado pelo direito e tecnologia nos dias atuais, era inimaginável há pouco anos. Ainda, há de ser levado em consideração que a LGPD, é recente, com apenas três anos de vigência, é notório que ainda há muito a ser aprimorado, tanto pelo ordenamento jurídico, quanto pelos programas de *compliance* digital, que tendem a ficar cada vez mais eficiente.

Conclui-se que o *compliance*, apesar do alto custo, possui inúmeras vantagens, para a empresa e para o titular, além de ser aplicável em qualquer empresa, independentemente do tamanho. Por outro lado, seus resultados não são exatos, também não é como se fosse uma receita pronta, apesar de existirem pilares norteadores, cada empresa terá sua própria necessidade que será analisada de acordo com os riscos da atividade empresarial.

Por fim, observou-se que por várias vezes a legislação brasileira foi inspirada nas estrangeiras, às vezes até forçadamente. Enquanto outros países são pioneiros em legislação de dados, o Brasil limita-se a inspirar-se neles. A LGPD, por ora, mostra-se suficiente, mas é sabido que as leis precisam acompanhar a evolução da sociedade; nesse caso específico, a legislação deve ser capaz de alcançar a tecnologia. Portanto, é necessário ficar mais que atento à tecnologia, pois se ontem a LGPD mostrava-se impossível e difícil de ser concretizada, através da evolução tecnológica, amanhã ou depois ela certamente pode se tornar atrasada se o legislador nada fizer. Assim, a legislação deve transmitir segurança, mas ainda encontra barreiras na insegurança causada pelo próprio ser humano, por isso, o programa de adequação deve ser dinâmico e atento aos riscos decorrentes das evoluções que a legislação ainda não foi capaz de regular.

REFERÊNCIAS

BOFF, Salete Oro; FORTES, Vinícius Borges. **A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil**. Sequência Estudos Jurídicos e Políticos, *[S. l.]*, v. 35, n. 68, p. 109–128, 2014. DOI: 10.5007/2177-7055.2013v35n68p109. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p109. Acesso em: 27 jun. 2023.

BOMBONATO, Lorrayne. **Contexto Histórico e Finalidade da Lei Geral de Proteção de Dados (LGPD).** IAPD**.** Disponível em: https://iapd.org.br/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/. Acesso em: 08 maio 2023.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União.** Brasília, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 02 abr. 2023.

BRASIL. Lei n° 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 12 set. 1990. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 20 jul. 2023.

BRASIL. Lei n° 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Brasília, 13 nov. 1997. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em: 22 jun. 2023.

BRASIL. Lei n° 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União.** Brasília, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 20 jul. 2023.

BRASIL. Lei n° 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, 10 jun. 2011. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 15 jul. 2023.

BRASIL. Lei n° 12.527, de 18 de novembro de 2021. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, 18 nov. 2011. **Diário Oficial da União.**

Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 15 fev. 2023.

BRASIL. Lei n° 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, 3 dez. 2012. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 22 jun. 2023.

BRASIL. Lei n° 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 24 abr. 2014. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 jul. 2023.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 15 ago. 2018. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 mar. 2023.

BRITTO, Vinícius; NERY, Carmen. **Internet já é acessível em 90,0% dos domicílios do país em 2020.** Agência IBGE notícias. 16 set. 2022. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021. Acesso em: 21 jun. 2023.

CAMARGO, Guilherme; FACHINETTI, Aline Fuke. **Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil**. Consultor Jurídico. 4 jul. 2021. Disponível em: https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados. Acesso em: 23 jun. 2023.

CANOTILHO, José Joaquim G.; MENDES, Gilmar F.; SARLET, Ingo W.; et al. Série IDP - Comentários à Constituição do Brasil. [Digite o Local da Editora]: Editora Saraiva, 2018. E-book. ISBN 9788553602377. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553602377/. Acesso em: 18 jul. 2023.

CAOVILLA, Renato; DUFLOTH, Rodrigo; PAZINE, Letícia. PROTEÇÃO DE DADOS PESSOAIS: DESAFIOS E IMPACTOS PRÁTICOS PARA AS ORGANIZAÇÕES. **Revista de Direito Recuperacional e Empresa**, vol. 12/2019, Abr - Jun/2019 DTR\2019\35342. Acesso em: 02 ago. 2023.

CAOVILLA, Renato; TIMM, Luciano Benetti. A estrutura de incentivos que conduz à conformidade. **JOTA**. 5 jun. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/coluna-da-abde/a-estrutura-de-incentivos-que-conduz-a-conformidade-05062017. Acesso em: 22 mar. 2023.

CARPENA, Heloisa. Consumidores internautas: da aplicabilidade do CDC à proteção de dados. **Jota**. 29 de out. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/consumidores-internautas-cdc-dados-29102020#sdfootnote1sym Acesso em: 11 jul. 2023.

CUEVA, Ricardo Villas Bôas. **A Insuficiente Proteção de Dados Pessoais no Brasil.** Capa. Nov. de 2016. Disponível em: https://core.ac.uk/download/pdf/211923195.pdf Acesso em: 05 jul. 2023

DALESE, Pedro; PALMEIRA, Mariana M. Os neurodireitos e a proteção de dados pessoais. **Jota**. 14 de jun. 2023. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/os-neurodireitos-e-a-protecao-de-dados-pessoais-14062023. Acesso em: 21 jul. 2023.

DECLARAÇÃO Universal dos Direitos Humanos. **UNICEF**. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 07 maio 2023.

DIAS, Fabiana. Terceira Revolução Industrial. **EDUCA+BRASIL.** 20 jul. 2020. Disponível em: https://www.educamaisbrasil.com.br/enem/historia/terceira-revolucao-industrial. Acesso em 02 de jun. 2023.

DONEDA, Danilo. A Proteção dos Dados Pessoais como Direito Fundamental. **Espaço Jurídico**. Jul/Dez. de 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 23 jun. 2023.

DONEDA, Danilo. **Iguais mas separados:** o Habeas data no ordenamento brasileiro e a proteção de dados pessoais. Caderno da Escola de Direito e Relações Internacionais. 2008. ISSN 16782933. Disponível em: https://portaldeperiodicos.unibrasil.com.br/index.php/cadernosdireito/article/view/2607/2180 Acesso em: 17 jul. 2023.

DONEDA, Danilo. O que está em jogo com a nova Autoridade Nacional de Proteção de Dados. **JOTA**. 13 de ago. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-que-esta-em-jogo-com-a-nova-autoridade-nacional-de-protecao-de-dados-13082018. Acesso em: 07 maio 2023.

FARIA, Felipe; SERPA, Alexandre; SIBILLE, Daniel. **Os pilares do programa de compliance.** São Paulo: LEC, 2020. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Os-pilares-do-programa-de-compliance.pdf. Acesso em: 02 ago. 2023.

FERRAÇO, Ricardo. Senado. **Parecer referente ao Projeto de Lei que estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados**

pessoais. Brasil, 2018. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://legis.senado.leg.br/sdleg-getter/documento?dm=7751914&ts=1594012451916&disposition=inline. Acesso em: 26 jul. 2023.

FRANÇA. Convenção 108 +. **Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal**. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em: 23 jun. 2023.

GARRIDO, Patricia P. **Proteção de dados pessoais:** comentários à lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2023. E-book. ISBN 9786555599480. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599480/. Acesso em: 23 jul. 2023.

GRINOVER, Ada P.; BENJAMIN, Antônio Herman de Vasconcellos E.; MARQUES, Cláudia L.; et al. **Código Brasileiro de Defesa do Consumidor.** São Paulo: Grupo GEN, 2022. E-book. ISBN 9786559645527. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559645527/. Acesso em: 21 jul. 2023.

HIRATA, Alessandro. Direito à privacidade. **ENCICLOPÉDIA JURÍDICA DA PUC**. 1 de abr. 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 07 maio 2023.

MENKE, Fabiano. Spiros Simitis e a primeira lei de proteção de dados no mundo. **MIGALHAS**. 19 de nov. de 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-protecao-de-dados-do-mundo. Acesso em: 08 maio 2023.

MIRANDA, Jorge. **Direitos fundamentais: uma perspectiva de futuro.** São Paulo: Grupo GEN, 2013. E-book. ISBN 9788522481095. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522481095/. Acesso em: 01 jun. 2023.

MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. **JOTA**. 14 de jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 20 mar. 2023.

MOUSSALLEM, Tarék Moysés; ROCHA, Cláudio Jannotti da; WERVLOET, Sabrina. A INCIDÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS E O COMPLIANCE NAS RELAÇÕES DE TRABALHO COMO INSTRUMENTOS PARA A PROTEÇÃO DE DADOS PESSOAIS DO TRABALHADOR NA 4ª REVOLUÇÃO INDUSTRIAL. **Revista dos Tribunais**, vol. 1022/2020, p. 255 – 270, DTR\2020\14377, Dez/2020. Acesso em: 28 jul. 2023.

OLIVEIRA, Ricardo Alexandre de. Lei Geral de Proteção de Dados Pessoais e seus Impactos no Ordenamento Jurídico. **Revista dos Tribunais**, vol. 998/2018, p. 241 – 261, DTR\2018\22546, Dez/2018. Acesso em: 25 jul. 2023.

ONU (org). **Declaração Universal dos Direitos Humanos.** 2020. Disponível em: https://brasil.un.org/ptbr/91601declaracaouniversaldosdireitoshumanos. Acesso em: 19 mar. 2022.

PESSÔA, Éder. Qual a importância do Código de Defesa do Consumidor? **Jornal JURID**. 10 de abr. 2023. Disponível em: https://www.jornaljurid.com.br/blog/auxilium/qual-a-importancia-do-codigo-de-defesa-do-consumidor. Acesso em: 14 jul. 2023.

PINHEIRO, Patrícia P. **Direito Digital.** São Paulo: Saraiva, 2021. E-book. ISBN 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 21 jul. 2023.

POLIDO, Fabrício Bertini Pasquot. LGPD e ANPD: Saiba o que são e entenda as diferenças entre a lei e o órgão. **JOTA**. 13 de abril de 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-anpd-saiba-o-que-sao-e-entenda-as-diferencas-entre-a-lei-e-o-orgao-13042022. Acesso em: 21 março 2023.

REINALDO FILHO, Demócrito. A Diretiva Europeia sobre proteção de dados pessoais: uma análise de seus aspectos gerais. **Revista Jus Navigandi**. Teresina, n. 3507, fev. 2013. Disponível em: https://jus.com.br/artigos/23669/a-diretiva-europeia-sobre-protecao-de-dados-pessoais. Acesso em: 5 maio 2023.

REIS, Beatriz de Felippe. A CULTURA DE COMPLIANCE EM MATÉRIA DE PROTEÇÃO DE DADOS E SUA ADOÇÃO NO ÂMBITO LABORAL. **Revista de Direito do Trabalho**, vol. 214/2020, p. 323 – 340, Nov - Dez/2020, DTR\2020\13289. Acesso em: 02 ago. 2023

ROCHA, Johnny. Lei Carolina Dieckmann completa 10 anos com baixa efetividade, avalia especialista. **Jota**. 02 de dez. 2022. Disponível em: https://www.jota.info/justica/lei-carolina-dieckmann-completa-10-anos-com-baixa-efetividade-avalia-especialista-02122022. Acesso em: 19 jul. 2023.

SANTOS, Fabíola M. de Almeida; TALIBA, Rita. Lei Geral de Proteção de Dados no Brasil e os Possíveis Impactos. **Revista dos Tribunais**, vol. 998/2018, p. 225 – 239, DTR\2018\22545, Dez/2018. Acesso em: 25 jul. 2023.

SANTOS, Maykon Adler Oliveira; ARAÚJO, Jeferson Sousa de; REGO, Ihgor Jean. A história Brasileira de proteção aos dados: o advento da lei geral de proteção de dados pessoais e a sua influência no acesso aos dados médicos no Brasil. **Revista Científica Multidisciplinar Núcleo do Conhecimento**. [S. l.] mar. 2021. v. 01, n. 12. Disponível em:

https://www.nucleodoconhecimento.com.br/lei/advento-da-lei. Acesso em: 10 maio 2023.

SCANDELARI, Gustavo B. **Compliance e Prevenção Corporativa de Ilícitos:** Inovações e Aprimoramentos para Programas de Integridade. São Paulo: Grupo Almedina (Portugal), 2022. E-book. ISBN 9786556276311. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556276311/. Acesso em: 28 jul. 2023.

SILVEIRA, Marco Antonio Karam. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SEU COMPLIANCE PARA EMPRESAS PRIVADAS. **Revista de Direito Civil Contemporâneo,** vol. 35/2023, p. 247 – 285, Abr – Jun/2023, DTR\2023\6856. Acesso em: 29 jul. 2023.

TOMASEVICIUS FILHO, Eduardo. **A Lei Geral de Proteção de Dados Brasileira**. Portugal: Grupo Almedina, 2021. E-book. ISBN 9786556271705. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556271705/. Acesso em: 19 jun. 2023.

TOMMASO, Raphael Di. Lei de proteção de dados completa 50 anos. **DIÁLOGOS DIREITOS DIGITAL E TECNOLOGIA**. 13 de out. 2020. Disponível em: https://digialogos.com.br/podcast/lei-de-protecao-de-dados-completa-50-anos. Acesso em: 08 maio 2023.

ZANINI, Leonardo E. de A. O Surgimento e o Desenvolvimento do *Right of Privacy* nos Estados Unidos. **Revista Brasileira de Direito Civil**. [S. l.] v. 3, n. 1. 2017. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Justitia%20n.204-206.21.pdf. Acesso em: 5 maio 2023.